IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

IN RE: DEALER MANAGEMENT SYSTEMS ANTITRUST LITIGATION	MDL No. 2817 Case No. 18-cv-00864
This Document Relates To: *Authenticom, Inc. v. CDK Global, LLC, et al.*, Case No. 1:18-cv-00868 (N.D. Ill.)	Hon. Robert M. Dow, Jr. Magistrate Judge Jeffrey T. Gilbert **PUBLIC-REDACTED**

PLAINITFF AUTHENTICOM, INC.'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT ON DEFENDANTS' COUNTERCLAIMS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES **Page(s)**

STATUTES

RULES AND REGULATIONS

OTHER AUTHORITIES

INTRODUCTION

Plaintiff Authenticom, Inc. ("Authenticom") has provided data integration services for dealers using Defendant The Reynolds & Reynolds Company's ("Reynolds") and Defendant CDK Global, LLC's ("CDK") DMS since 2004. CDK and Reynolds were aware of and consented to access by Authenticom and other data integrators for more than a decade. CDK's CEO proclaimed that allowing data integrators to access the DMS was the "dealer's right," and as late as August 2013, CDK championed the rights of data integrators such as Authenticom: [redacted] Indeed, CDK acquired and operated two of the largest data integrators – Digital Motorworks Inc. ("DMI") in 2002 and IntegraLink in 2010 – and even founded an industry coalition called Open Secure Access whose primary purpose was to advocate for continued DMS access by data integrators. And although Reynolds publicly criticized data integrators, there is no factual dispute that, in practice, Reynolds consented to that access on a massive scale. [redacted] Reynolds did so because dealers and software vendors needed and relied on the services provided by data integrators, and Reynolds had no feasible alternative. Tellingly, Reynolds itself used Authenticom's data integration services for its non-DMS software applications for more than a decade – including on CDK's and its own DMS.

Notwithstanding these undisputed facts, and their own identical conduct, CDK and Reynolds now contend that Authenticom was an unlawful computer "hacker" during this entire period, and they assert a laundry list of counterclaims seeking more than ***$7 billion*** in damages. CDK and Reynolds brought these counterclaims only after their agreement to block data

integrators became the subject of antitrust litigation and government investigation. The claims are makeweight and unworthy of trial.

I. CDK's and Reynolds's counterclaims depend on the premise that Authenticom obtained *unauthorized* access to their DMS. But those counterclaims founder on CDK and Reynolds's own contracts with their dealer customers. Those contracts unambiguously authorized dealers' "agents" to access and use the DMS. Now that discovery is complete, there is no genuine factual dispute that Authenticom was the dealers' "agent." The evidence undisputedly shows that Authenticom acted on dealers' behalf in facilitating the provision of dealer data stored on the DMS to software application vendors so that those vendors could create software applications that assist the dealers in their retail operations. Dealers had the ability to control all aspects of Authenticom's service, including which data Authenticom could access, the third-party software vendors to whom Authenticom would provide data access, the precise data fields that each third-party software vendor would be allowed to access, and the frequency of that data access. [redacted]

II. CDK and Reynolds assert that Authenticom violated the Digital Millennium Copyright Act ("DMCA") by circumventing three access controls: (1) CAPTCHA prompts that required reentry of text displayed on the screen, (2) Yes/No prompts that required answering "Yes" that the user was authorized, and (3) CDK's and Reynolds's disabling of login credentials used by data integrators. These claims cannot survive summary judgment for four independent reasons.

A. Even assuming Defendants' technological measures qualify for statutory protection (and they do not), Authenticom did not "circumvent" any of them. The statute defines "circumvention" as "avoid[ing], bypass[ing], deactivat[ing], or impair[ing]" the technological

measure. 17 U.S.C. § 1201(a)(3)(A). As to CAPTCHA and the Yes/No prompts, Authenticom did none of these things; to the contrary, the evidence is undisputed that it *satisfied* the prompts by providing the information requested (which appears on the face of the prompt). As to the disablement of login credentials, the evidence shows that all Authenticom did was obtain new login credentials from dealers or to have dealers re-enable existing credentials when Defendants disabled credentials that they believed were being used by Authenticom. This was not an act of "circumvention"; it was exactly what CDK and Reynolds told dealers they could legitimately do.

B. The DMCA applies only to technological measures that "control[] access to a [copyrighted] work." 17 U.S.C. § 1201(a). CDK and Reynolds assert the copyrighted work is their DMS software, consisting of the executable code for that software and the visual elements of that software that are displayed while the software runs (that is, the look-and-feel of the software). However, the technological measures did not control access to the executable code because Authenticom never encountered any of the three technological measures before any access to or running of that executable code. The Sixth Circuit and Ninth Circuit have refused to apply the DMCA in identical circumstances. CDK's and Reynolds's DMCA claims also do not survive with respect to the visual elements of their DMS software. They have failed to present necessary expert evidence that the visual elements (for example, the menus and other screen elements) were creative works entitled to copyright protection as opposed to purely functional choices not entitled to copyright protection.

C. Defendants' DMCA claim requires that Authenticom have circumvented a "technological measure" that "effectively controls access to a [copyrighted] work." 17 U.S.C. § 1201(a)(1)(A). A technological measure "effectively controls access" only if it "requires the application of information, or a process or a treatment, with the authority of the copyright owner,

to gain access to the work." *Id.* § 1201(a)(3)(B). As the statute's text indicates, the essential characteristic of a technological measure that "effectively controls access" is that the measure attempt to preclude access to a copyrighted work by those who lack authority to access that work. As the drafters of the law put it, such a measure must "require[ ] the use of a 'key' provided by a copyright owner to gain access to a work." Report of the House Commerce Comm., H.R. Rep. No.105-551, Part 2, at 39 (2d Sess. 1998). A quintessential example is a login and password provided to an authorized user.

CDK's and Reynolds's CAPTCHA and Yes/No prompts do not fit within the statutory definition because neither attempts to prevent access at all. Indeed, completely unlike the "key" envisioned by the law's drafters, it is undisputed that the CAPTCHA and Yes/No prompts provide the user – on their face – with all the information necessary to satisfy the prompts. [redacted] CDK's and Reynolds's CAPTCHA and Yes/No prompts were the equivalent of an "unlocked" door that anyone could open without "break[ing] in"; the DMCA does not cover such measures. *See Dish Network L.L.C. v. World Cable Inc.*, 893 F. Supp. 2d 452, 465 (E.D.N.Y. 2012).

CDK's and Reynolds's disabling of login credentials likewise fail the requirement that the measure require "the application of information, or a process or a treatment . . . to gain access to the work." By design, CDK's and Reynolds's monitoring programs did not require Authenticom to do anything to gain access to the DMS. Those measures allowed access to the DMS and only flagged certain accounts – after access had been gained – for possible disabling at a later time.

D. Under *Assessment Techs. of WI, LLC v. WIREdata, Inc.*, 350 F.3d 640 (7th Cir. 2003), Authenticom's access to the DMS was fair use as a matter of law. Where a database owner

has no copyright interest in the underlying data stored in the database – which CDK and Reynolds have conceded – it is fair use for outside parties to obtain that data even if doing so requires incidental use of the database owner's software; it would be "appalling" for CDK and Reynolds to "secrete the data" (in which they have no copyright interest) in their copyrighted programs. *Id.* at 641-42. The lack of any copyright violation negates DMCA liability. *See Chamberlain Grp., Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178, 1192-93 (Fed. Cir. 2004).

III. CDK's and Reynolds's counterclaims are partially time barred. Their counterclaims are based on discrete instances of access by Authenticom, and they seek damages for access as far back as May 2013 for Reynolds and August 2014 for CDK. But CDK's and Reynolds's counterclaims have statutes of limitations as short as two years, such that CDK and Reynolds may not pursue claims based on access many years ago.

IV. The counterclaims fail for several additional, independent reasons.

A. Private litigants may pursue Computer Fraud and Abuse Act ("CFAA") claims only where "the conduct" – here, each instance of access by Authenticom – meets one of several statutory severity thresholds. CDK and Reynolds base their claims on the statutory threshold that requires them to show each instance of access for which they bring suit caused more than $5,000 of loss; that statutory test prevents them from aggregating several instances of access (a "related course of conduct") to meet that threshold. 18 U.S.C. § 1080(c)(4)(A)(i)(I). Instead of analyzing loss for each instance of access as required by the CFAA, CDK's and Reynolds's damages expert aggregated the loss from tens of thousands of different instances of access. CDK and Reynolds therefore have no competent evidence to satisfy the severity threshold in the CFAA.

B. CDK's trade secret claims fail because CDK has not identified any trade secret that was misappropriated by Authenticom. This Court previously noted that CDK's allegations about

the nature of its trade secrets – a vague reference to "forms, accounting rules, tax tables, and proprietary tools and data compilations," Dkt. 229, CDK Counterclaims ¶¶ 23, 115, 127 – were not "robust." *In re DMS Antitrust Litig.*, 362 F. Supp. 3d 558, 574-75 (N.D. Ill. 2019). Discovery has shown them to have no substance. CDK's own expert provided no competent evidence that CDK's DMS contains any trade secrets. [redacted]

C. California's Unfair Competition Law ("UCL") only allows plaintiffs to "seek[ ] the return of money or property" that "defendants took directly from plaintiff." *Korea Supply Co. v. Lockheed Martin Corp.*, 63 P.3d 937, 943 (Cal. 2003). But it is undisputed that neither CDK nor Reynolds gave Authenticom any money or property. Rather, Authenticom received compensation for its services from the software vendors to whom it provided data access on behalf of the dealer (and for a shorter period, from the dealer itself). Defendants lack any evidence of damages – an essential element of their claim – because their damages expert does not even attempt to quantify damages caused by any violation of the UCL.

D. CDK's and Reynolds's common-law trespass to chattels claims fail because there is no evidence that Authenticom's access impaired the functioning of their DMS – which is an essential element of their claims. As to liability, Defendants' employees testified they were unaware of any incident in which Authenticom impaired the functioning of their system, except for one incident that was resolved in less than a day in 2009 – well outside the statute of limitations. And as to damages, even setting aside the lack of reliability of CDK's expert opinion (which purports to extrapolate an unrepresentative sample of *four dealers on a single day* to thousands of dealers over a three-and-a-half-year period), he does not purport to measure damages associated

with *impairment* of the DMS's functioning, which is what trespass to chattels requires. *See Ticketmaster Corp. v. Tickets.com, Inc.*, 2000 WL 1887522, at *4 (C.D. Cal. Aug. 10, 2000) (evidence of "hits" to a computer system are insufficient to establish trespass where "there is no showing that the use interferes to any extent with the regular business" of the system owner) *aff'd*, 2 F. App'x 741 (9th Cir. 2001).

E. CDK and Reynolds may not pursue their unjust enrichment claim against Authenticom for accessing their DMS because they are already pursuing a breach of contract claim against dealers for the same supposed injury: access to the DMS by Authenticom without payment to CDK or Reynolds. Well-settled law precludes an unjust enrichment claim for a subject governed by a contract, even where that contract is with a third party.

F. CDK's fraud claim fails because CDK instituted the prompt that it claims elicited false responses from Authenticom for the very purpose of eliciting what CDK believed to be false responses from Authenticom. Having received exactly what it expected, CDK cannot establish reasonable reliance on those representations. Reynolds's fraud claim fails because it has failed to provide evidence of any representation (false or not).

V. CDK's and Reynolds's damages expert, Professor Daniel Rubinfeld, and CDK's security expert – who purported to determine the number of DMCA statutory violations – have made egregious errors that require exclusion of their testimony. *See* Dkts. 861, 871. Once that testimony is properly excluded, CDK and Reynolds have no competent proof of damages, requiring dismissal of any request for statutory or compensatory damages.

BACKGROUND

I. Automobile Dealership Software

Car dealerships use Dealer Management System ("DMS") software to run their businesses. This software automates many business functions, including payroll, inventory, customer relationship management, service, and other areas at the dealership. *See* Plaintiffs' Statement of Fact ("PSOF") ¶ 1. The DMS includes a database that stores data central to dealership operations, such as service appointments, customers, and inventory. *See id.* ¶ 2. Much of that data is generated by car dealerships during their regular business operations. *See id.* ¶ 3. For example, the inventory data stored in the DMS includes the dealership's inventory available for sale; the customer data stored in the DMS includes information about customers that have transacted with the dealership; and the service data stored in the DMS includes records of past and future service appointments at the dealership. It is widely recognized in the automotive industry – including by CDK and Reynolds – that dealers have a right to control who should have access to most, if not all, data stored in the DMS. *See id.* ¶ 4; Ex. 95, PX 1726 at CDK-3122863 (CDK: "[A] dealership fundamentally owns the data in its DMS, and dealers should control who accesses their data and how it's used"); PSOF ¶ 5 Ex. 73, PX 636 (Reynolds: "You own your data and choose who you allow access to it.").

CDK and Reynolds have been the two largest DMS providers for at least three decades. Their combined market share has consistently been more than 70% when measured by dealership count. *See* PSOF ¶ 7. Their market share is even higher – more than 90% – when measured by the share of new car sales of the dealerships that use their DMS. *See id.*

Dealers also rely on other non-DMS software to run their business operations. These applications are tailored to specific functions within the dealership, such as customer relationship management ("CRM"), inventory, accounting, and parts and service. *See id.* ¶ 9. For many of

these applications to function properly, they need access to the dealer's data that is stored on the DMS. *See id.* ¶ 10.

II. Data Integration

Software vendors access data stored on the DMS through data integration services. *See id.* ¶ 11. These data integration services may be provided by the DMS provider itself or by independent data integrators. *See id.* ¶ 12. In either case, dealers authorize these data integrators to access the dealer's data stored on the DMS and to provide software vendors with access to that data. *See id.* ¶ 14; [redacted].

Data integration services may be provided through several different methods, including (1) a "push" or "batch-delivery" process where data is periodically transferred to a third party, (2) an application programming interface ("API"), which allows for programmatic data access, and (3) "user emulation" software that emulates human interaction with the DMS. For the "user emulation" method, the dealer provides DMS login credentials to the data integrator, which then uses those credentials to access the DMS and provide the data integration service. *See* PSOF ¶ 16; [redacted] Both CDK's and Reynolds's DMS give dealers the ability to create additional user accounts and to specify the permissions for each account – that is, what data that can be accessed by the account. *See* PSOF ¶ 17. Three of the largest data integrators are Authenticom, which is

an independent data integrator, and Digital Motorworks, Inc. ("DMI") and IntegraLink, which are owned by DMS provider CDK. *See id.* ¶ 14.[1]

A. Authenticom

Authenticom was an American success story before the events at issue in this litigation decimated its business and caused it to lay off two-thirds of its workforce in 2018. Authenticom was founded in 2002 by entrepreneur Steve Cottrell, who at first ran the business out of his home. *See id.* ¶ 19. Authenticom grew to 120 employees in La Crosse, Wisconsin. *See id.* ¶ 20. In a July 2015 speech, President Barack Obama heralded Authenticom as "one of America's fastest growing private companies," known for giving its employees not only well-paying jobs but also an equity stake in the company's success. *See id.* ¶ 21 (speech available at www.youtube.com/watch?v=Bfzu9kd5HU8). At its height in early 2015, Authenticom provided data integration services to nearly 500 software vendors across 15,000 dealer rooftops. *See id.* ¶ 22. Authenticom's customers included (and continue to include) CDK and Reynolds. *See id.* ¶¶ 114, 116; [redacted]

During the relevant time period, Authenticom accessed the DMS through "user emulation" (also known as "screen scraping" or "terminal emulation").[2] Dealers created login credentials for

[1] Data integrators may also offer other services such as standardizing data or correcting errors within the data. *See* PSOF ¶ 13.

[2] *Screen Scraping*, Techopedia, *available at* https://www.techopedia.com/definition/16597/screen-scraping ("Screen scraping usually refers to a legitimate technique used to translate screen data from one application to another. . . . Screen scraping is sometimes referred to as terminal emulation.").

Authenticom's use in the same way that dealers would give their own employees login credentials. *See id.* ¶ 24. Authenticom used those credentials to access the DMS in the same way as a dealer employee. *See id.* ¶ 27. That is, the software would "emulate" a dealer employee's use of the DMS, allowing for automated extraction of or writing data to the DMS. *See id.* Dealers could limit the data that Authenticom could access by restricting the permissions associated with the credentials given to Authenticom. *See id.* ¶ 26. The dealer could also revoke Authenticom's login credentials at any time. *See id.* ¶ 25. Authenticom would not access any dealer data without that dealer's express, written authorization. *See id.* ¶ 23; Ex. 2, Korp. Decl. ¶ 25 ("Several of our vendors use Authenticom to pull the dealerships data. I have expressly and specifically authorized Authenticom to perform this service.").

The dealer controls all aspects of Authenticom's data integration service. PSOF ¶¶ 30, 33. The dealer decides which software vendors can receive its data through Authenticom, *see id.* ¶ 33; the dealer controls the types of data that each software vendor is allowed to access through Authenticom's service, *see id.* ¶ 35; and the dealer controls the timing and frequency that each software vendor is allowed to access data through Authenticom, *see id.* ¶ 36.

In September 2013, Authenticom launched its DealerVault product to give dealers even greater control over Authenticom's data integration service. PSOF ¶ 29. DealerVault includes an online portal that allows dealers to select the specific data fields that software vendors should be allowed to access, plus the schedule on which such access should be allowed. *See id.* ¶ 36; [redacted] DealerVault

also allows dealers the ability to see records of the data sent to or received from software vendors. *See* PSOF ¶ 37. As CDK's and Reynolds's (since replaced) security expert Eric Rosenbach testified upon seeing a demonstration of DealerVault: "[W]hen we talk about transparency, DealerVault itself, I think, is good. That's an impressive piece of technology. It does give the dealer transparency on data that's there and where it's going." *Id.* ¶ 38; Ex. 11, PI Hearing Tr. 1-P-134:23-135:1.[3]

Dealers laud the control that DealerVault gives them. *See* PSOF ¶ 39; [redacted] Ex. 14, PI Hearing Tr. 2-A-6:14-18 (Wayne Fitkin, Dealer IT director: DealerVault is "an incredibly exceptional product . . . . It's the best thing I have ever seen because for once I had a single pane of glass to see every third-party vendor that was receiving data."). They consider their relationship with Authenticom to be a principal-agent relationship. *See* PSOF ¶ 42; [redacted]

CDK and Reynolds likewise have recognized the control that DealerVault gives to dealers. PSOF ¶¶ 43-44. [redacted]

[3] *See also* PSOF ¶ 38; Ex. 12, PI Hearing Tr. 2-P-168:20-169:2 (Howard Gardner, CDK's Head of Data Services: conceding that it is "implausible" that dealers using "Authenticom's DealerVault" do not "know where [their] data is going"; "Authenticom, my guess, is they are doing a good job explaining where the data is going.").

[redacted][4]

B. DMI and IntegraLink

Defendant CDK owns two data integrators, DMI and IntegraLink. PSOF ¶ 14. Both data integrators have relied on login credentials provided to them by dealers. *Id.* ¶ 46. [redacted]

[4] CDK and Reynolds frequently expressed concern about the competitive threat that DealerVault posed. [redacted]

[redacted]

[redacted]

III. DMS Contracts

The relationships between CDK and Reynolds and their dealer customers are governed by two sets of contracts, CDK's Master Services Agreement and Reynolds's Master Agreement.

A. CDK's Master Services Agreement

CDK's Master Services Agreement ("MSA") grants the "Client" – the dealer – a license to use the DMS. PSOF ¶ 54; Ex. 15, MSA § 1. The MSA further allows the "Client" to "make available" the "CDK Products" – which includes the DMS[5] – and any associated "screen displays" to the "Client's" "employees and agents" but not to "third parties." *Id.* § 6(D). The MSA has included these provisions since at least 2008. *See* PSOF ¶ 55.

[redacted]

[5] [redacted]

B. Reynolds's Master Agreement

[redacted]

IV. Data Access Policies

Since approximately 2006, Reynolds has publicly criticized the use of non-Reynolds data integrators, has taken steps to block data integrators, and has encouraged dealers to use its own data integration service, the Reynolds Certified Interface ("RCI"). *See* PSOF ¶¶ 67-68. Nonetheless, Reynolds dealers used non-Reynolds data integrators for many years with Reynolds's knowledge and consent. [redacted] Industry participants – [redacted] – did not understand Reynolds to forbid dealers from authorizing independent data integrators to access the Reynolds DMS. [redacted]

[redacted]

In contrast to Reynolds, CDK historically supported dealers' use of data integrators. *See* PSOF ¶ 72; [redacted] CDK sought to [redacted]. CDK's CEO Steve Anenen summarized CDK's position as: "I don't know how you can ever make the opinion that the data is yours to govern and to preclude others from having access to it when in fact it's really the data belonging to the dealers. As long as they grant permission, how would you ever go against that wish? I don't understand that." PSOF ¶ 73; Ex. 84, PX 933.[6] CDK maintained this position into 2013. [redacted]

[6] *See also* Ex. 89, PX 1179 at CDK-0012546 ("That is the dealer's right. We have no right to tell them they can't do that"); Ex. 93, PX 1647 at CDK-3122887 (CDK Senior VP: Access by data integrators "is no different than a dealership allowing access to their system by their accounting team for the purpose of an annual audit. There are many justified reasons for a dealer to provide approved access to the data and the systems they are paying their DMS vendor for each month.").

In addition to its public stance, CDK was itself the largest provider of data integration services due to its acquisitions of DMI (in 2002) and IntegraLink (in 2010). *See supra* pp. 13-15. CDK also joined an industry coalition called Open Secure Access to promote dealer control over DMS access. *See* PSOF ¶ 75; Ex. 86, PX 1035 (founding press release); Ex. 95, PX 1726 at CDK-3122863 (CDK CEO: "[T]he principles that [OSA] has endorsed are exactly the same principles that we hold near and dear to our own business philosophy: that a dealership fundamentally owns the data in its DMS, and dealers should control who accesses their data and how it's used."). One of the tenets of the Open Secure Access coalition was that dealers should be allowed to grant DMS access to data integrators. *See* PSOF ¶ 77; Ex. 87, PX 1036 (listing as a "key principle": "Third parties that have dealer permission to utilize a dealer's data should be allowed to access the data through their own efforts or through the services of an independent company."). [redacted]

V. Blocking Data Integrators

In 2009, Reynolds began implementing measures intended to make access by data integrators more difficult. *See* PSOF ¶ 78. Initially, these measures did not meaningfully affect data integrators. *Id.* ¶ 79. [redacted]

[redacted]

CDK did not implement measures that disrupted access by data integrators until the summer of 2016. *See* PSOF ¶ 87. [redacted]

Reynolds and CDK allege they employed three technological measures that frustrated access by data integrators: CAPTCHA (both Reynolds and CDK), Yes/No Prompts (only CDK), and disabling user credentials (both Reynolds and CDK). *See* Dkt. 229, CDK Counterclaims ¶¶ 83-95; Dkt. 225, Reynolds Counterclaims ¶¶ 50-53.

CAPTCHA. CAPTCHA stands for Computer Automated Program for Telling Computers and Humans Apart. The CAPTCHA employed by CDK and Reynolds displayed – with varying degrees of distortion – text on the screen that the user had to re-enter in order to proceed. *See* PSOF ¶¶ 81, 90. Reynolds first began deploying simple "ASCII" CAPTCHA – CAPTCHA that was itself displayed as text characters on the screen – around 2010, *see id.* ¶ 81 (exemplar image), and deployed graphical CAPTCHA – an image with distorted text – by 2012, *see id.* ¶ 82 (exemplar image). CDK did not deploy CAPTCHA until October 2017 – after it had already been sued for antitrust violations. *See id.* ¶ 90.

Authenticom responded to the CAPTCHA by entering the text that was displayed on the screen; it has never bypassed a CAPTCHA without entering the correct response. *See* PSOF ¶ 91; Ex. 54, [redacted] Authenticom determined the correct response by several means. [redacted][7]

Yes/No Prompts. In June 2016, CDK implemented this prompt:

```
login: heidi
Password:
Last login: Thu Mar 24 09:10:10 from 139.126.150.113
A RAID EVENT has been reported in the raid event directory.
It is important to notify your CRR of this RAID EVENT as soon as possible.
The CDK Global DMS is for authorized Dealer personnel only.
Use or access by unauthorized third parties is prohibited.
Those using this system without authorization will be denied
access and may have their services revoked.
Enter "YES" to confirm you are an authorized dealer employee
in order to continue,  enter "NO" to exit this program.
yes
```

[7] [redacted]

[redacted] And within a day after first encountering the prompt, Authenticom did modify its software to respond "Yes." *See id.* ¶ 102. This was the only method used by Authenticom to respond to the "Yes/No" prompt. *See id.* ¶ 103.

Disabling User Credentials. In 2012, Reynolds began deactivating login credentials that it suspected were being used by data integrators, and CDK followed suit in late 2016. *See id.* ¶¶ 83, 87. Authenticom's login credentials were disabled only after they had been used by Authenticom to gain access to the DMS. *See id.* ¶ 84. Authenticom tried several methods to avoid having its login credentials disabled, but the only successful method was for the dealer to either re-enable the login credentials or to create new login credentials for Authenticom. *See id.* ¶ 85. For CDK dealers, Authenticom developed a script called Profile Manager that automated the process of re-enabling Authenticom's login credentials. *See id.* ¶ 104. The dealer ran Profile Manager, and Profile Manager only used tools that CDK made available to the dealer in its DMS to manage login credentials. *See id.* ¶¶ 105-06. Further, both CDK and Reynolds told dealers that they could re-enable login credentials for data integrators that had been disabled, though neither guaranteed the dealer that CDK and Reynolds would stop disabling the credentials. [redacted]

[redacted]

VI. Counterclaims

CDK and Reynolds assert that dealers are contractually prohibited from granting data integrators like Authenticom access to their DMS, and that neither CDK nor Reynolds authorizes such access. *See* Dkt. 229, CDK Counterclaims ¶¶ 3, 8, 35 & n.46, 71-75, 82; Dkt. 225, Reynolds Counterclaims ¶¶ 2, 8, 10-11, 32, 54-60. CDK and Reynolds further claim to have instituted various technological measures designed to block data integrators, and that Authenticom has circumvented these measures. *See* Dkt. 229, CDK Counterclaims ¶¶ 7, 41, 83-93; Dkt. 225, Reynolds Counterclaims ¶¶ 8, 10-11, 52-53, 71-80. CDK and Reynolds also allege that their software is a creative work entitled to copyright protection. *See* Dkt. 229, CDK Counterclaims ¶ 21 ("terminal program"); Dkt. 225, Reynolds Counterclaims ¶¶ 30-31. They claim that each time Authenticom accesses their DMS, Authenticom creates copies of the DMS code. *See* Dkt. 229, CDK Counterclaims ¶ 45; Dkt. 225, Reynolds Counterclaims ¶¶ 31, 81-82.

CDK and Reynolds assert the following claims against Authenticom. The conversion claims have already been dismissed. *See In re DMS Antitrust Litig.*, 362 F. Supp. 3d at 575-78.

Claim	CDK	Reynolds
Violation of the Computer Fraud And Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(2)(C) for accessing Reynolds's and CDK's DMS without authorization	Yes (Count I)	Yes (Count I)
Violation of the Digital Millenium Copyright Act ("DMCA"), 17 U.S.C. § 1201(a)(1)(A), (a)(2), (b)(1), for circumventing technological access controls and offering products primarily designed to circumvent technological access controls	Yes (Count II)	Yes (Count III)
Violation of the Defend Trade Secrets Act, 18 U.S.C. § 1836(b), for misappropriating CDK's trade secrets	Yes (Count III)	No
Violation of the Wisconsin Computer Crimes Act ("WCCA"), Wis. Stat. § 943.70(2)(a), for accessing Reynolds and CDK's DMS without authorization	Yes (Count IV)	Yes (Count IV)

Claim	CDK	Reynolds
Violation of the Wisconsin Uniform Trade Secrets Act, Wis. Stat. § 134.90, for misappropriating CDK's trade secrets	Yes (Count V)	No
Violation of the California Comprehensive Computer Data Access and Fraud Act ("CCCDAF"), Cal. Penal Code § 502(c), for accessing CDK's DMS without authorization	Yes (Count VI)	Yes (Count V)
Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, for unlawful access to CDK's and Reynolds's DMS	Yes (Count VII)	Yes (Count X)
Tortious interference with CDK's and Reynolds's contracts with dealers	Yes (Count VIII)	Yes (Count VI)
Trespass to chattels for accessing CDK's and Reynolds's DMS without authorization	Yes (Count IX)	Yes (Count VII)
Conversion for using CDK's and Reynolds's servers without authorization	Previously Dismissed	Previously Dismissed
Unjust enrichment for benefits received from access to CDK's and Reynolds's DMS	Yes (Count XI)	Yes (Count IX)
Fraud for representing that Authenticom was authorized to access CDK's and Reynolds's DMS	Yes (Count XII)	Yes (Count XI)
Copyright infringement for making copies of Reynolds's DMS software and screen layouts	No	Yes (Count II)

ARGUMENT

"Under Rule 56 of the Federal Rules of Civil Procedure, a court 'shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.'" *Ellis v. CCA of Tenn. LLC*, 650 F.3d 640, 646 (7th Cir. 2011) (quoting Fed. R. Civ. P. 56(a)). "A summary judgment motion is appropriately granted against a party who fails to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial." *Id.* (internal quotation marks omitted). "To survive summary judgment, a non-movant must be able to show that a reasonable jury could return a verdict in its favor – metaphysical doubt as to the material facts does not create a genuine issue for trial." *Id.*

I. All of the Counterclaims Fail Because Authenticom Had Authorization To Access CDK's And Reynolds's DMS

CDK's and Reynolds's contracts with dealers unambiguously authorize agents of the dealer to access the DMS, *see infra* Part I.A., and there is no genuine dispute of material fact that Authenticom acted as the agent of the dealer in accessing the dealer's DMS, *see infra* Part I.B. These undisputed facts result in the dismissal of Reynolds's and CDK's counterclaims because each counterclaim hinges on Authenticom's access being unauthorized. *See infra* Part I.C.

A. The DMS Contracts Unambiguously Allow Access By Dealers' Agents

1. Both CDK's and Reynolds's contracts with its dealers unambiguously allow "agents" of the dealer to access and use the DMS – like Authenticom, as explained *infra* Part I.B. CDK's MSA allows dealers to "make available" the DMS and its "screen displays" to "employees and agents." Ex. 15, MSA § 6(D). Reynolds's Master Agreement provides that dealers and their [redacted] As this Court previously held, "the phrase 'agents and employees' is not

ambiguous"; the only question is "whether Authenticom falls within the scope of that language." *In re DMS Antitrust Litig.*, 362 F. Supp. 3d 558, 556 n.2 (N.D. Ill. 2019) (citing *Hernandez ex rel. Gonzalez v. Tapia*, 2010 WL 5232942, at *7 (N.D. Ill. Dec. 15, 2010) ("The phrase 'agents and employees' is not ambiguous" and should be interpreted according to its "plain meaning.")).

The provisions of CDK's and Reynolds's contracts with dealers that impose limitations on the access and use of the DMS by "third parties" do not apply to "agents" like Authenticom. CDK's Master Services Agreement states that the dealer "shall not allow access . . . by any *third parties* except as otherwise permitted by this Agreement." Ex. 15, MSA § 6(D). Similarly, Reynolds's Master Agreement states dealers may not "disclose or provide access" to the DMS "to any *third party*," Ex. 19, Master Agreement § 1 – and the Customer Guide states dealers must "not copy, reproduce, distribute, or in any way disseminate or allow access to or by *third parties*," Ex. 137, REYMDL00012246 at 267. But both sets of agreements make clear that dealers' "agents" are not included within the category of "third parties" that may not be granted access: Section 6(D) of CDK's Master Services Agreement expressly allows "agents" but not "third parties" to access the DMS, Ex. 15, MSA § 6(D), and Section 1 of the Reynolds Master Agreement expressly allows [redacted] To read the term "third party" to encompass "agents" would create an internal conflict and would effectively nullify the provision expressly granting dealers permission to give access to their agents. *See BKCAP, LLC v. CAPTEC Franchise Tr. 2000-1*, 572 F.3d 353, 362 (7th Cir. 2009) ("[C]ourts must . . . give effect to every word, phrase, and clause in a contract and avoid an interpretation that would render any part of the contract surplusage or nugatory" (alterations in original)); *Thompson v. Gordon*, 948 N.E.2d 39, 47 (Ill. 2011) ("A court will not interpret a contract in a manner that would nullify or render

provisions meaningless, or in a way that is contrary to the plain and obvious meaning of the language used"); *Transtar Elec., Inc. v. A.E.M. Elec. Servs. Corp.*, 16 N.E.3d 645, 651-52 (Ohio 2014) ("[C]ourts should not interpret contracts in a way that renders at least one clause superfluous or meaningless." (brackets omitted)).

Indeed, the "rule" for "copyright licens[es]" – like the dealer contracts – is that "absent express contrary agreement, a license to use technology encompasses an 'implied license' to have the technology used by a third party on the licensee's behalf." Nimmer & Dodd, *Modern Licensing Law* 6:19 (2013); *Estate of Hevia v. Portrio Corp.*, 602 F.3d 34, 45-46 (1st Cir. 2010) ("When . . . there is no indication that a license-granting copyright owner has restricted the licensee's ability to use third parties in implementing the license, the license is generally construed to allow such delegation."); *Avaya, Inc. v. Telecom Labs, Inc.*, 2014 WL 97335, at *6 n.26 (D.N.J. Jan. 7, 2014) ("[T]he prevailing construction of licensing agreements [is to] allow third-party use for the licensee's benefit."). For example, in *Automation by Design, Inc. v. Raybestos Prods Co.*, 463 F.3d 749 (7th Cir. 2006), Automation by Design and Raybestos entered into a licensing agreement that allowed Raybestos to "duplicate the design" of a machine but not to "transfer" the license. *Id.* at 754. The court held that Raybestos's agent inherited the same rights under the license agreement as Raybestos: "Once Raybestos secured the rights to duplicate the designs . . . , it could hire another party to manufacture parts for it if Raybestos lacked the tools or skills to do so itself." *Id.* at 757. These principles for interpreting licensing agreements apply fully here: Authenticom – the dealer's agent – inherited the dealer's right to use and access the DMS.

Neither CDK's Master Services Agreement nor Reynolds's Master Agreement places any pertinent restrictions on how dealers' agents access or use the DMS. In particular, Section 6(B) of CDK's Master Services Agreement does not prohibit user emulation software that automates

tasks that would otherwise be performed manually. That provision states the dealer "IS NOT AUTHORIZED TO CAUSE OR PERMIT ANY THIRD PARTY SOFTWARE TO ACCESS THE CDK DEALER MANAGEMENT SYSTEM EXCEPT AS OTHERWISE PERMITTED BY THIS AGREEEMENT." PSOF ¶ 55. CDK has confirmed that dealers are permitted to use software that they own or operate to "automate[ ]" use of the DMS. *Id.* ¶ 109; Ex. 94, PX 1673. The prohibition on allowing "*third party* software" therefore does not apply to a dealer's own software. Nor does that provision apply to software created by a dealer's agent (for example, programmers hired by the dealer) because of the distinction that the agreement draws between "agents" and "third parties." *See Chicago Home for Girls v. Carr*, 133 N.E. 344, 346 (Ill. 1921) ("Words used in one sense in one part of a contract are, as a general rule, deemed to have been used in the same sense in another part of the instrument, where there is nothing in the context to indicate otherwise."); *Commissioner v. Keystone Consol. Indus., Inc.*, 508 U.S. 152, 159 (1993).

At the motion to dismiss stage, this Court held that Section 6(B) – along with CDK's other allegations that Authenticom's access was "unauthorized" – made it plausible that the MSA did not authorize "Authenticom to access CDK's DMS with its software" even if Authenticom was dealers' agent. *DMS Antitrust Litig.*, 362 F. Supp. 3d at 569. That ruling was based on the allegation that CDK had implemented "security measures . . . to prevent Authenticom's automated access," *id.*, but discovery has shown those efforts were haphazard and taken only after a decade of CDK supporting automated access by data integrators. *See supra* pp. 17-18. It does not control on this more complete record. *See Melton v. Five Four Corp.*, 2000 WL 97568, at *5 (N.D. Ill. Jan. 25, 2000) (court's disposition of legal issues on motion to dismiss "does not control the analysis" at the summary judgment stage and taking "a fresh look at the sufficiency of the legal claims in light of the factual record"); *Thornton v. Hamilton Sundstrand Corp.*, 54 F. Supp. 3d

929, 938 n.5 (N.D. Ill. 2014) ("A denial of a motion to dismiss does not preclude the Court from considering the same argument on summary judgment.").

For the same reason, a similar prohibition in the Reynolds Customer Guide on "install[ing] Other Matter on the Equipment" and "connect[ing] Other Matter to Licensed Matter" does not prohibit use of user emulation software by the dealer or its agents. *See* Ex. 20, Customer Guide at -265. "Other Matter" is defined to be "any software product, database, or other materials provided to you *by a third party*, which is capable of functioning on or with Equipment." Ex. 21, Defined Terms, at 679 (emphasis added). This provision therefore restricts only "connecting" software provided to the dealer by "third parties," not created by the dealer itself or provided to the dealer by its agents.

2. Even if there were ambiguity in the DMS contracts, summary judgment is still warranted due to the "undisputed extrinsic evidence," *Tranchitella v. Bank of Ill. in DuPage*, 199 B.R. 658, 664 (N.D. Ill. 1996) – specifically, the parties' course of performance. "Generally speaking, the practical interpretation of a contract by the parties to it for any considerable period of time before it comes to be subject of controversy is deemed of great, if not controlling, influence." *Old Colony Tr. Co v. City of Omaha*, 230 U.S. 100, 118 (1913); *see Moriarty v. Svec*, 164 F.3d 323, 332 (7th Cir. 1998) (such evidence "highly relevant"); *Teamsters Indus. Emps. Welfare Fund v. Rolls-Royce Motor Cars, Inc.*, 989 F.2d 132, 137 (3d Cir. 1993) ("Evidence of a course of conduct is particularly compelling when it occurs over a substantial time period."); *see Lincoln Elec. Co. v. St. Paul Fire & Marine Ins. Co.*, 210 F.3d 672, 686 (6th Cir. 2000); *NanoeXa Corp. v. Univ. of Chi.*, 2011 WL 1399264, at *3-4 (N.D. Ill. Apr. 13, 2011) (Illinois law).[8]

[8] *See also Fed. Armored Exp., Inc. v. Harris Tr. & Sav. Bank*, 1995 WL 124254, at *3 (N.D. Ill. Mar. 20, 1995) ("[W]here . . . the parties themselves have placed a construction on the

For more than a decade – until the conspiracy between CDK and Reynolds – nearly every automobile dealership relied on one or more data integrators, such as Authenticom, DMI, or IntegraLink. [redacted] CDK and Reynolds were aware of the prevalence of data integrators: CDK supported the use of data integrators as the "dealer's right," PSOF ¶ 72, and to this day, [redacted] For its part, Reynolds – despite its public objections to the use of data integrators – [redacted] CDK and Reynolds also gave dealers the practical ability to use data integrators by giving dealers the unfettered ability to manage the user credentials for their DMS – an ability that CDK and Reynolds never took away from the dealers. *See id.* ¶¶ 16-18.[9]

---

language by their conduct, that construction should be adopted by the court"); *Wald v. Chicago Shippers Ass'n*, 529 N.E.2d 1138, 1147 (Ill. App. Ct. 1988) ("Further, where the terms of a contract are doubtful or uncertain and the parties to it have, by their own conduct, placed a construction upon it which is reasonable, such construction will be adopted by the courts.").

[9] The practice in the DMS industry mirrors the practice in the broader enterprise resource planning ("ERP") software industry, of which the DMS industry is a subset. *See* PSOF ¶ 111. [redacted]

Dealers likewise testified that they understood data integrators to be their agents and that DMS access by their agents was allowed under their contracts with CDK and Reynolds. *See* PSOF ¶ 42; [redacted] Ex. 11, PI Hearing Tr. 1-P-196:24-197:1. And Authenticom is aware of no instance in which CDK or Reynolds filed suit against a dealer to prevent a dealer from allowing its agents to use the DMS, despite this occurring every day at thousands of dealers over more than a decade.[10]

On this record, CDK and Reynolds cannot credibly argue that the intention of CDK, Reynolds, and the dealers all this time was to prohibit the use of data integrators when the uniform and long-sustained course of conduct was to the contrary. CDK apparently does not even believe its own argument: in late 2017 – after this litigation began – CDK began trying to modify its contracts with dealers to remove the "agent" language. *See* Dkt. 229, CDK Counterclaims ¶¶ 73, 75 & n.52. The Court should grant summary judgment that dealers' agreements with CDK and Reynolds allowed the dealers to authorize their agents to use and access the DMS. *See Ross Univ. Sch. of Med., Ltd. v. Brooklyn-Queens Health Care, Inc.*, 2012 WL 6091570, at *14 (E.D.N.Y. 2012) (granting summary judgment despite ambiguous contract language because the extrinsic evidence (including course of conduct) "overwhelmingly supports [the movant's] interpretation"); *Faulkner v. Nat'l Geographic Soc'y*, 452 F. Supp. 2d 369, 381 (S.D.N.Y. 2006) (granting summary judgment based on undisputed extrinsic evidence; "[u]nlike the subjective intent or *post hoc*

10 [redacted]

conclusions of contracting parties, the parties' course of dealing throughout the life of a contract is highly relevant to determining the meaning of the terms of the agreement").[11]

B. Authenticom Was The Dealers' Agent

Authenticom acted as the dealers' agent when facilitating provision of data access to a dealer's software vendors because Authenticom was "acting on behalf of [the dealer]" and "subject to control of" the dealer. *Lang v. Lions Club of Cudahy Wisconsin, Inc.*, 2020 WL 1056905, at *5 (Wis. Mar. 5, 2020); *Arsand v. City of Franklin*, 264 N.W.2d 579, 583 (Wis. 1978) (an agent is "a person authorized by another to act on his account and under his control.").[12] The agency question turns on whether the principal has "the right to control the conduct" at issue. *Lang*, 2020 WL 1056905, at *7; *Giese v. Montgomery Ward, Inc.*, 331 N.W.2d 585, 597 (Wis. 1983) (agency relationship established where the principal had the "right to control" the agent's "performance of the task" and "benefited from its performance.").

Summary judgment is appropriate here because the undisputed evidence shows that dealers had the right to control all aspects of Authenticom's provision of data integration services. *Lang*, 2020 WL 1056905, at *1 (granting summary judgment when there was no genuine factual dispute regarding existence of agency relationship); *Automation by Design*, 463 F.3d at 757 (same); *Select Creations, Inc. v. Paliafito Am., Inc.*, 911 F. Supp. 1130, 1150-52 (E.D. Wis. 1995) (same). The

---

[11] Any ambiguities in the contracts should also be resolved against CDK and Reynolds – the drafter of the form agreements used with dealers. *See Covinsky v. Hannah Marine Corp.*, 903 N.E. 2d 422, 427 (Ill. App. Ct. 2009); *Michael A. Gerard, Inc. v. Haffke, Michael A. Gerard, Inc. v. Haffke*, 2013 WL 267296, at *3 (Ohio Ct. App. Jan. 24, 2013).

[12] The law of Wisconsin – where Authenticom is based, enters into contracts with dealers, and performs data integration services on behalf of dealers, governs the agency analysis. *See NUCOR Corp. v. Aceros Y Maquilas de Occidente, S.A. de C.V.*, 28 F.3d 572, 582 (7th Cir. 1994) (agency choice of law determined by the forum with the "most significant relationship to the parties and the transaction." (citing Restatement (Second) of Conflicts, §§ 291-292 (1971)).

dealer controls the access permissions of the user credentials that the dealer provides to Authenticom, *see* PSOF ¶ 32; Ex. 104, CDK-0012573 § 3.4 (DealerVault Terms & Conditions: "DealerVault shall only extract the Dealership Data that the Dealership permits DealerVault to extract"); the dealers can revoke those credentials at any time, *see* PSOF ¶ 25; the dealer controls which data Authenticom accesses, *see id.* ¶¶ 26, 35; the dealer controls to which third-party software vendors Authenticom provides data access, including the precise data fields to which each third party has access, *see id.* ¶¶ 33-35, 39-40; the dealer controls the frequency with which Authenticom provides that data access, *see id.* ¶ 36; and the dealer may audit each instance of data access by a third-party software vendor through Authenticom's services, *see id.* ¶ 37.

The Wisconsin Supreme Court's recent decision in *Lang* is on all fours. In *Lang*, the Lions Club hired a third-party vendor to provide music for a 2012 festival, including laying the necessary electric cords. *See* 2020 WL 1056905, at *1. The Lions Club did not provide any "specific instructions" to the vendor but "had the right to control how the electronic and electrical cords were placed." *Id.* at *2. The Wisconsin Supreme Court held an agency relationship existed as a matter of law, because the vendor "was subject to the Lions Club's right to control" the conduct at issue – the placement and covering of the electrical wires. *Id.* at *8. The Court distinguished *Westmas v. Creekside Tree Serv., Inc.*, 907 N.W.2d 68, 77 (Wis. 2018) – on which this Court relied at the motion-to-dismiss stage, *In re DMS Antitrust Litig.*, 362 F. Supp. 3d at 567 (N.D. Ill. 2019) – explaining that, in *Westmas*, the alleged principal "merely had the right to expect a result as opposed to the right to control" the work. *Lang*, 2020 WL 1056905 at *6. Here – as in *Lang* and unlike *Westmas* – dealers did not merely have a right to expect that Authenticom would facilitate

data access by third-party software vendors; dealers had the right to precisely control the provision of data access to third-party software vendors.[13]

The Terms and Conditions between Authenticom and its dealers – which stated that the parties would be "independent contractors" and "do not intend" for there to be an "employment agency, joint venture, or partnership relationship," Ex. 104, Terms and Conditions § 10.4 – do not change the outcome. The *substance* of the parties' relationship governs "[r]egardless of how the two parties chose to define their relationship for remuneration, tax, employment law, or tort liability purposes." *Automation by Design*, 463 F.3d at 757; *see* Restatement (Third) of Agency § 1.02 ("Whether a relationship is characterized as agency in an agreement between parties or in the context of industry or popular usage is not controlling."); *MJ & Partners Rest. Ltd. v. Zadikoff*, 10 F. Supp. 2d 922, 932 (N.D. Ill. 1998) ("[T]he existence of an agency relationship is determined based on the actual practices of the parties, and not merely by reference to a written agreement."). At the motion to dismiss stage – and in the absence of any evidence or allegations whether "dealers reserved the right to control the details of [Authenticom's] work" – this Court gave some weight to the contract's characterization of the relationship. *See DMS Antitrust Litig.*, 362 F. Supp. 3d at 567-68. However, now the developed factual record establishes that, with respect to data integration services, Authenticom acts as the dealers' agent. In addition, as the Wisconsin

---

[13] [redacted] Key dealer groups – including the California New Car Dealers Association – have touted the control that Authenticom's DealerVault product gives dealers over their data. *See id.* ¶ 41.

Supreme Court recently held in *Lang*, a contract defining a party as an "independent contractor" is consistent with that party being an "agent." 2020 WL 1056905, at *6.[14]

C. Each of the Counterclaims Fails As a Matter of Law In Light of the Undisputed Evidence That Authenticom's Access Was Authorized

Each of CDK's and Reynolds's counterclaims fails because each depends on proof that Authenticom's access to the DMS was unauthorized.

The Computer Fraud And Abuse Act, the Wisconsin Computer Crimes Act, and the California Comprehensive Computer Data Access And Fraud Act. Each of these computer access statutes prohibits access "without authorization" or "without permission." The CFAA makes it unlawful to "intentionally access[ ] a computer *without authorization*," 18 U.S.C. § 1030(a)(2)(c); the WCCA prohibits "[a]ccessing computer programs" "willfully, knowingly *and without authorization*," Wis. Stat. § 943.70(2); and the CCDFA prohibits "[k]nowingly access[ing] *and without permission* . . . mak[ing] use of any . . . computer system," Cal. Penal Code § 502(c)(2) (all emphases added). The WCCA and CCDFA are interpreted in accord with the CFAA. *See Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010); *c.f. Maxpower Corp. v. Abraham*, 557 F. Supp. 2d. 955, 962-63 (W.D. Wis. 2008) (interpreting WCCA's provisions as analogous to CFAA).

Consistent with its plain meaning, "'authorization' means 'permission or power granted by an authority.'" *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009) (quoting Random House Unabridged Dictionary, 139 (2001)). As explained above, dealers' contracts with

---

[14] *See* Restatement (Second) of Agency § 14N (independent contractor may be agent); *Automation by Design*, 463 F.3d at 757 (holding agency relationship existed as a matter of law despite parties "specifically defin[ing] their relationship as that of independent contractors and not agents"); *Select Creations*, 911 F. Supp. at 1152 (whether third party is an "independent contractor is irrelevant to the agency inquiry" because "independent contractors . . . may be agents as well").

Defendants expressly permitted access by dealers' agents, and the undisputed evidence shows that Authenticom was such an agent. Accordingly, summary judgment on Defendants' CFAA, WCCA, and CCDFA claims must be granted because Authenticom's access was not "without authorization" or "without permission." *See EarthCam, Inc. v. OxBlue Corp.*, 49 F. Supp. 3d 1210, 1231-32 (N.D. Ga. 2014) (granting summary judgment for defendant who received access credentials from a third party, where the license agreement between the plaintiff and the third party did not prevent the third party "from sharing their passwords"), *aff'd*, 703 F. App'x 803 (11th Cir. 2017) (per curiam); *ATPAC, Inc. v. Aptitude Sols., Inc.*, 2010 WL 177901, at *5 (E.D. Cal. Apr. 29, 2010) (dismissing CFAA claim as a matter of law where defendant received the access code from a third party and where there were no allegations that the third party "wrongfully provided" the access code to the defendant); Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1178-79 (2016) ("If the agent accesses the account on the account holder's behalf, the agent is acting in the place of the account holder and is authorized.").[15]

This Court previously stated in its motion to dismiss ruling that Defendants' claims were plausible because even if the DMS contracts "allowed dealers to give Authenticom access to CDK's DMS, Authenticom's access to the DMS over CDK's express objection would still violate the CFAA and parallel state-law statutes" because CDK had allegedly revoked that permission. *DMS Antitrust Litig.*, 362 F. Supp. 3d at 569-70. As a legal matter, however, the permission CDK gave dealers was a matter of binding contract; CDK and Reynolds were not entitled to withdraw it unilaterally without amending those contracts, and there is no evidence of any such amendment.

[15] *See also Amphenol Corp. v. Paul*, 993 F. Supp. 2d 100, 110 (D. Conn. 2014) (defendant who was "authorized to access" the computer in question "did not violate the CFAA"); *Océ N. Am., Inc. v. MCS Servs., Inc.*, 748 F. Supp. 2d 481, 486 (D. Md. 2010) (no CFAA violation where defendant "was authorized to access the website and information located there").

The evidence thus does not support CDK's revocation allegation. *See Melton*, 2000 WL 97568, at *5 (disposition of legal issues on motion to dismiss "does not control the analysis" at the summary judgment stage and taking "a fresh look at the sufficiency of the legal claims in light of the factual record.").[16]

Indeed, interpreting the CFAA, WCCA, and CCDFA to impose liability where a computer owner unilaterally revoked permission that had been previously given by contract would be contrary to law. The CFAA, WCCA, CCDFA are modern trespass statutes. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1000 (9th Cir. 2019) ("[T]he CFAA is best understood as an anti-intrusion statute. . . . We therefore look to whether the conduct at issue is analogous to 'breaking and entering.' "). Because these statutes "cover[ ] a field formerly governed by the common law" (trespass) they should be "interpreted consistently with the common law" of trespass. *Samantar v. Yousuf*, 560 U.S. 305, 320 (2010); *see Theofel v. Farey-Jones*, 359 F.3d 1066, 1072-73 (9th Cir. 2004) (interpreting the Stored Communications Act, which also prohibits "access[ ] without authorization," 18 U.S.C. § 2701(a)(1), in accord with "the common law of trespass").

Under the common law, if a property owner grants access to his or her property by contract, that property owner cannot unilaterally revoke that access and sue for trespass: "One who effectively consents to conduct of another intended to invade his interests cannot recover in an action for tort for the conduct or harm resulting from it. . . . Upon termination of consent its

---

[16] At oral argument in the appeal of the preliminary injunction, Judge Easterbrook addressed a separate question: whose "authorization" matters for purposes of CFAA liability. 18 U.S.C. § 1030(a)(2). Authenticom argued then that the CFAA should be construed so that the "authorization" of the dealer – "the owner of the data" – was dispositive. Dkt. 256-7, at 49:21-51:2. Authenticom does not presently pursue this argument in this motion. Rather, Authenticom now argues that CDK and Reynolds gave their "authorization" by entering into binding contracts that allowed dealers' agents to access their DMS.

effectiveness is terminated, *except as it may become irrevocable by contract or otherwise*." Restatement (Second) of Torts § 892A (emphasis added); *see id.* § 167 (applying this general principle to trespass). For example, if the lease between a landlord and tenant allows the tenant to invite guests to the property, the landlord has no action for trespass against the invited guest given that prior binding contractual commitment. *See, e.g., Oregon v. Schneider*, 265 P.3d 36, 38 (Or. Ct. App. 2011).[17]

The rule of lenity also counsels against an interpretation of the term "without authorization" that allows a party to unilaterally revoke their previously given contractual consent. Where there are competing "plausible interpretations of a criminal statute" like the CFAA, "the rule of lenity requires [the Court] to adopt the defendant's construction." *United States v. Valle*, 807 F.3d 508, 523 (2d Cir. 2015) (interpreting CFAA). This "ensures that criminal statutes will provide fair warning of what constitutes criminal conduct." *Id.* It would be a surprise to many if, after making a binding contractual commitment that access to a computer system would be allowed, the system operator could unilaterally breach that contract and thereby transform contractually authorized access into a criminal act punishable by up to 10 years in prison. *See* 18 U.S.C. § 1030(c).[18]

---

[17] The result is the same under intellectual property law. A sublicense is a valid defense to a claim of infringement by the licensor if the licensee was permitted by the license to grant the sublicense. *See Spinelli v. NFL*, 96 F. Supp. 3d 81, 121-22 (S.D.N.Y. 2015) ("[I]t is well established that use of a copyrighted work within the scope of the license is non-infringing as a matter of law . . . and a valid license . . . immunizes the license from a charge of copyright infringement. . . . The same holds true for a sublicensee's use that has been authorized by a licensee."); *Major League Baseball Promotion Corp. v. Colour-Tex, Inc.*, 729 F. Supp. 1035, 1041 (D.N.J. 1990) ("Under copyright law, a person is innocent of infringement if he possesses a sublicense issued by a licensee upon the due authority of the copyright owner.").

[18] *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016) is not to the contrary. There, the Court held that access was unauthorized after Facebook "expressly rescinded" permission to access, but unlike here, there was no binding contractual commitment by Facebook that such access would be allowed. *See id.* at 1067.

DMCA. The DMCA prohibits circumvention of technological measures protecting works "without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A) (emphasis added). Those with authority to access the work are "immune from § 1201(a)(1) circumvention liability." *Chamberlain*, 381 F.3d at 1204; *see Ticketmaster L.L.C. v. Prestige Entm't, Inc.*, 306 F. Supp. 3d 1164, 1174 (C.D. Cal. 2018) ("legitimate users . . . do not violate the DMCA"). Accordingly, just as with the CFAA, the undisputed evidence that Authenticom was the dealers' agent, and thus was authorized under the plain terms of the dealers' DMS contracts with Defendants, dooms CDK's and Reynolds's DMCA claims.

Tortious Interference. The tortious interference claims are based on Authenticom allegedly inducing dealers to breach their DMS contracts by requesting that the dealers provide Authenticom with access to CDK's and Reynolds's DMS. *See* Dkt. 225, Reynolds Counterclaims ¶ 152; Dkt. 229, CDK Counterclaims ¶ 153. The claims necessarily fail because dealers' grant of authorization to Authenticom to access the DMS on their behalf was not a violation of the dealers' DMS contracts. *See Welch v. Moore Bus. Forms, Inc.*, 394 N.W.2d 316 (Wis. Ct. App. 1986) (tbl.) (tortious interference claim must be dismissed where the plaintiff "failed to establish that any contractual right was violated") (per curiam).

Trespass to chattels. Trespass requires "intentional[ ] intermeddl[ing] with a chattel which is in the possession of another," "without a consensual or other privilege to do so." *Wisconsin Telephone Co. v. Reynolds*, 87 N.W.2d 285, 288 (Wis. 1958) (quoting Restatement (First) of Torts, § 218). Here again, Authenticom and the dealers *had* CDK's and Reynolds's consent because the dealers' DMS contracts permitted their agents to access the DMS on their behalf. As with the CFAA, that contractual authorization defeats any claim of common-law trespass. *See* Restatement (Second) of Torts § 252 ("One who would otherwise be liable to another

for trespass to a chattel or for conversion is not liable to the extent that the other has effectively consented to the interference with his rights"); *id.* § 253 ("One who would otherwise be liable for another for trespass to a chattel . . . is not liable to the extent that he has acted with the consent of a third person with power to give consent effective as to the other.").

California UCL. The UCL prohibits "any unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200. Both CDK and Reynolds assert claims under the "unlawful" prong, while CDK also asserts a claim under the "unfair" prong. *See* Dkt. 229, CDK Counterclaims ¶¶ 145-146; Dkt. 225, Reynolds Counterclaims ¶¶ 175-179. The "unlawful" prong "borrows violations of other laws and treats them as unlawful practices." *Cel-Tech Commc's, Inc. v. Los Angeles Cellular Tel. Co.*, 973 P. 2d 527, 539-40 (Cal. 1999); *accord In re Vaccine Cases*, 134 Cal. App. 4th 438, 456 (2005). Because Authenticom's access was authorized and did not violate any law, that access was not "unlawful" under the UCL. *See Asencio v. Miller Brewing Co.*, 283 F. App'x 559, 562 (9th Cir. 2008) ("[B]ecause [plaintiff's] claim was dismissed[,] . . . [s]he cannot proceed with her claim that [defendant's] conduct was 'unlawful' under UCL."). CDK's claim under the "unfair" prong similarly fails because that prong covers only "conduct that threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws because its effects are comparable to or the same as a violation of the law, or otherwise significantly threatens or harms competition." *Cel-Tech*, 973 P.2d at 544; *id.* at 541 ("Courts may not simply impose their own notions of the day as to what is fair or unfair.").

Trade secrets. The Defend Trade Secrets Act ("DTSA") and the Wisconsin Uniform Trade Secrets Act ("WUTSA") prohibit "acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means." 18 U.S.C. § 1839(5). The statute expressly states that "lawful means of acquisition" are not "improper

means." *Id. at* § 1839(6); Wis. Stat. § 134.90(2) (same); *see also ConFold Pac., Inc. v. Polaris Indus., Inc.*, 433 F.3d 952, 959 (7th Cir. 2006) (conduct not actionable under DTSA "without either a tort or a breach of contract"); *see Sapienza v. Trahan*, 2019 WL 348820, at *12 (W.D. La. Jan. 28, 2019) (information lawfully received not misappropriated under DTSA). Given Defendants' contractual authorization of dealers' agents, there is no genuine dispute that any access by Authenticom was done by lawful means.

Copyright. "[T]he existence of a license . . . creates an affirmative defense to a claim of copyright infringement." *Muhammad-Ali v. Final Call, Inc.*, 832 F.3d 755, 761 (7th Cir. 2016). The DMS contracts – which allowed access and use by dealers' agents – provided a license for any access or use of CDK's or Reynolds's intellectual property by Authenticom.

Unjust enrichment. Unjust enrichment "requires a wrongful taking or appropriation of others' property to one's own use." *Major Mat Co. v. Monsanto*, 969 F.2d 579, 585 (7th Cir. 1992) (quoting *Abbott Labs. v. Norse Chem. Corp.*, 147 N.W.2d 529, 541 (Wis. 1967)); *see also Fail Safe LLC v. A.O. Smith Corp.*, 762 F. Supp. 2d 1126, 1133-34 (E.D. Wis. 2011). There can be no "wrongful taking or appropriation" when CDK and Reynolds voluntarily authorized access to their DMS. *Id.* at 1132 (a party cannot claim unjust enrichment for benefits voluntarily conferred on another); Restatement (Third) Restitution and Unjust Enrichment § 2 cmt. d (same); *cf. Indiana Lumbermens Mut. Ins. Co. v. Reinsurance Results, Inc.*, 513 F.3d 652, 656 (7th Cir. 2008) ("One who voluntarily confers a benefit on another, which is to say in the absence of a contractual obligation to do so, ordinarily has no legal claim to be compensated.") (applying Indiana law).

Fraud. These claims are based on the allegation that Authenticom allegedly misrepresented that it had authorization to access CDK's and Reynolds's DMS. *See* Dkt. 229, CDK Counterclaims ¶¶ 174-175; Dkt. 225, Reynolds Counterclaims ¶ 181. There was no

misrepresentation as a matter of law because Authenticom was authorized to access CDK's and Reynolds's DMS.

II. Summary Judgment Should Be Granted On Defendants' DMCA Counterclaims

The DMCA is a criminal statute that makes it unlawful to (1) "circumvent" a technological measure that (2) "effectively controls access to" (3) a copyrighted work. 17 U.S.C. § 1201(a)(1)(A); *see id.* § 1204(a) (punishable by up to 10 years in prison). CDK and Reynolds lack evidence to support all three of these requirements. In addition, they fail the requirement that there be a nexus between the circumvention of an access control and a copyright violation.[19]

A. Authenticom Did Not "Circumvent" The Technological Measures

CDK's and Reynolds's DMCA claims fail because Authenticom did not "circumvent" the technological measures; it complied with them in the same manner as an ordinary, authorized user. Even assuming Authenticom's access was "unauthorized," that alone would not be a DMCA violation absent "circumvention" of an access control. *Navistar, Inc. v. New Baltimore Garage, Inc.*, 2012 WL 4338816, at *5 (N.D. Ill. Sept. 20, 2012); *see I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004) ("Unlike the CFAA, a cause of action under the DMCA does not accrue upon unauthorized and injurious access *alone*; rather

---

[19] CDK and Reynold have also asserted claims under 17 U.S.C. § 1201(a)(2) and 17 U.S.C. § 1201(b), both of which prohibit the "manufacture, import, offer to public, provi[sion], or [trafficking]" of certain circumvention devices. However, CDK's and Reynolds's experts do not calculate damages for any alleged violations of these provisions. [redacted] In any case, Authenticom did not violate these provisions for the same reasons that it did not violate 17 U.S.C. § 1201(a)(1).

the DMCA targets the *circumvention* of digital walls guarding copyrighted material." (internal quotation marks omitted; emphasis in original)). The DMCA "expressly limit[s]" "circumvention" to "descrambling a work, decrypting an encrypted work, or otherwise avoiding, bypassing, removing, deactivating, or impairing" a technological measure. *See Navistar*, 2012 WL 4338816, at *5; 17 U.S.C. § 1201(a)(3)(A). This list of prohibited acts "impl[ies] that a person circumvents a technological measure only when he affirmatively performs an action that disables or voids the measure that was installed to prevent them from accessing the copyrighted work." *Healthcare Advocates, Inc. v. Harding, Early, Follmer & Frailey*, 497 F. Supp. 2d 627, 644 (E.D. Pa. 2007).[20]

CAPTCHA and Yes/No Prompts. Authenticom did not circumvent any CAPTCHA prompt or any Yes/No prompt. The evidence is undisputed that Authenticom complied with those prompts by supplying the requested information. *See* PSOF ¶¶ 91, 103. That is not circumvention as a matter of law. This Court's decision in *Navistar, Inc. v. New Baltimore Garage, Inc.*, 2012 WL 4338816 (N.D. Ill. Sept. 20, 2012) is dispositive. There, New Baltimore Garage gave passwords to a third party who used the passwords to access Navistar's computer system without Navistar's authorization. *Id.* at *1. This Court held that the use of those "password[s] to access a copyrighted work, even without authorization, does not constitute 'circumvention' under the DMCA because it does not involve descrambling, decrypting, or otherwise avoiding, bypassing, removing, deactivating, or impairing a 'technological measure.'" *Id.* at *5. Because a valid password was used to respond to the password prompt (even if by an unauthorized user), there was no "avoid[ing] or bypass[ing] the deployed technological measure in the measure's gatekeeping capacity." *Id.* at *4 (internal quotation marks omitted). This Court's holding is supported by the

[20] Because the DMCA is a criminal statute, the rule of lenity requires application of a construction favoring the accused violator in the case of any ambiguity. *See supra* p. 37.

great weight of authority. *See Avaya, Inc. v. Telecom Labs, Inc.*, 2012 WL 13035096, at *5-7 (D.N.J. May 1, 2012) (no circumvention because "[r]egardless of how [defendant] obtained usernames or passwords . . . it *used* those logins to access" the system).[21]

Navistar and similar decisions compel summary judgment in favor of Authenticom for the CAPTCHA and Yes/No prompts. Just as the third party in *Navistar* complied with the password prompt by supplying the requested information (a valid username and password), Authenticom supplied the response requested by the CAPTCHA prompt (the displayed characters) and requested by the Yes/No prompt ("Yes"). *See* PSOF ¶¶ 91, 99; [redacted] There is no evidence that Authenticom ever "disabled," "avoided," or "bypassed" the prompts.

At the motion-to-dismiss stage, this Court (and a couple others) allowed DMCA claims based on CAPTCHA to proceed to discovery. This Court did so upon crediting (as it needed to) CDK's allegation that Authenticom "crack[ed]" the CAPTCHA, thus "circumvent[ing] the CAPTCHA," CDK Counterclaim ¶ 92. *See In re DMS Antitrust Litig.*, 362 F. Supp. 3d at 571-72 ("Authenticom's use of an automated program to bypass CDK's use of a CAPTCHA does avoid

[21] *See also R. Christopher Goodwin & Assocs., Inc. v. SEARCH, Inc.*, 2019 WL 5576834, at *3 (E.D. La. Oct. 29, 2019); *Digital Drilling Data Sys. LLC v. Petrolink Servs., Inc.*, 2018 WL 2267139, at *14-15 (S.D. Tex. May 16, 2018); *Adobe Sys. Inc. v. A&S Elecs., Inc.*, 2015 WL 13022288, at *8 (N.D. Cal. Aug. 19, 2015); *Burroughs Payment Sys., Inc. v. Symco Grp., Inc.*, 2011 WL 13217738, at *4-5 (N.D. Ga. Dec. 13, 2011); *Flagstone Island Gardens, L.L.C. v. Ser*, 2011 WL 13223685, at *2-3 (S.D. Fla. Sept. 13, 2011); *Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678 690-92 (D. Md. 2011); *Aeropost Int'l Servs., Inc. v. Aerocasillas, S.A.*, 2011 WL 13174672, at *5-6 (S.D. Fla. Mar. 31, 2011); *R.C. Olmstead, Inc. v. CU Interface, LLC*, 657 F. Supp. 2d 878, 888-89 (N.D. Ohio 2009); *Egilman v. Keller & Heckman, LLP*, 401 F. Supp. 2d 105, 113-14 (D.D.C. 2005); *I.M.S.*, 307 F. Supp. 2d at 532-33.

and/or bypass the technological measures taken by CDK to prevent the use of automated programs."). Because the allegations of "cracking" or other circumvention have been disproven, summary judgment is now warranted.

User ID blocking. CDK and Reynolds claim that Authenticom circumvented CDK's and Reynolds's efforts to block its user IDs by trying to avoid detection and by re-enabling the user IDs once blocked. *See* Ex. 149, Expert Report of Scott Tenaglia ("Tenaglia Rep."), at 8-9; Ex. 148, Expert Report of Edward Stroz ("Stroz Rep."), ¶¶ 89, 117. But they present no evidence that any of Authenticom's efforts to avoid detection were successful. Their experts do not quantify the number of times Authenticom supposedly successfully avoided detection; they do not address the issue at all. *See* Ex. 159, Stroz Rep. ¶¶ 72, 103, 105. Thus, at best, CDK and Reynolds have mustered evidence of "attempts" to avoid detection. But the DMCA does not provide a private cause of action for "attempted circumvention." The statute covers only the act of "circumvent[ing] a technological measure." 17 U.S.C. § 1201(a); *compare id.* § 1203(c) (providing damages in a civil suit for "violations" and not "attempted violations"), *with* 18 U.S.C. § 1030(b) (providing liability for one who "attempts" to violate the CFAA); *see also United States v. Chi Tong Kuok*, 671 F.3d 931, 941 (9th Cir. 2012) ("We have long recognized that '[t]here is no general federal "attempt" statute. A defendant therefore can only be found guilty of an attempt to commit a federal offense if the statute defining the offense also expressly proscribes an attempt.'" (quoting *United States v. Hopkins*, 703 F.2d 1102, 1104 (9th Cir. 1983))).

Nor was it a violation for Authenticom to request that their dealer customers re-enable login credentials or to provide new credentials to Authenticom. It is undisputed that CDK's and Reynolds's DMS were designed to allow dealers to manage the login credentials to their DMS. *See* PSOF ¶¶ 16-18. Moreover, CDK and Reynolds told dealers that they could re-enable any

credentials that had been disabled if the dealer desired to do so. *See id.* ¶¶ 86, 89. Using the features of the DMS for their designed purpose – and at the direction of CDK and Reynolds – is not "circumventing" an access control. Nor is there any evidence that Authenticom in any way impeded the continued functioning of CDK's and Reynolds's "Suspicious ID Monitoring" measures: to the contrary, CDK and Reynolds claim those measures continued to function by disabling Authenticom's logins. *See* Dkt. 229, CDK Counterclaims ¶ 89; Dkt. 225, Reynolds Counterclaims ¶ 53. There was therefore no circumvention of those measures. *See Healthcare Advocates*, 497 F. Supp. 2d at 644 (circumvention only where defendant "disables" or "voids" a technological measure).

Finally, CDK (but not Reynolds) attempts to hold Authenticom liable for supplying a program to dealers (Profile Manager) to automate the manual process of re-enabling credentials for Authenticom. *See* Dkt. 229, CDK Counterclaims ¶ 89; Ex. 148, Stroz Rep., App'x C ¶¶ 36-50. Profile Manager merely automated the permissible process of a dealer employee re-enabling disabled credentials. *See* PSOF ¶ 104; Ex. 165, Clements Decl. ¶ 5. Profile Manager did not affect the continued functioning of CDK's "Suspicious ID monitoring" in any way. *See id.* Therefore, Profile Manager was also not "circumvention" for the same reasons that a dealer employee manually taking the same steps was not circumvention.

In all events, CDK may not hold Authenticom liable for each instance in which Profile Manager was run by a dealer, even if the program did not re-enable any of Authenticom's credentials. [redacted]

[redacted] CDK's attempt to artificially inflate its damages is indefensible and should be rejected as a matter of law.

B. The Technological Measures Did Not Protect Copyrighted Works

The DMCA covers only circumvention of technological measures for "a work protected" by copyright. 17 U.S.C. § 1201(a); *see Lexmark Int'l, Inc. v. Static Controls Components, Inc.*, 387 F.3d 522, 550 (6th Cir. 2004). CDK and Reynolds assert that the three technological measures protected their DMS software, meaning the software's (1) executable code, and (2) visual elements. *See* Dkt. 225, Reynolds Counterclaims ¶¶ 30-31, 70, 81-82, 118-121; Dkt. 229, CDK Counterclaims ¶ 45.

Executable code. CDK's and Reynolds's technology measures did not prevent access to the executable code. The CAPTCHA, Yes/No, and login prompts appeared only *after* the executable code had been accessed and run. *See* PSOF ¶ 108; Ex. 155, Expert Rebuttal Report of Nancy Miracle ("Miracle Rebuttal Rep."), ¶¶ 12-17. Any entity – including Authenticom – could have obtained the executable code and ran that code without encountering the technological measures. *See* PSOF ¶ 108; Ex. 165, Clements Decl. ¶ 13. These technological measures therefore did not "effectively control access" to the executable code because they did not require Authenticom to do *anything* prior to "gain[ing] access to the work." 17 U.S.C. § 1201(a)(3).

The Sixth and Ninth Circuits have held that there is no DMCA claim under the same circumstances. In *Lexmark*, 387 F.3d at 546, the Sixth Circuit held an "authentication sequence" did not "control access" to printer software because anyone who purchased the printer could "read the literal code" of the software "directly from the printer memory, with or without the benefit of the authentication sequence." *Id.* at 546; *see id.* at 547 ("Just as one would not say that a lock on

the back door of a house 'controls access' to a house whose front door does not contain a lock . . . , it does not make sense to say that this provision of the DMCA applies to otherwise-readily-accessible copyrighted works."). The Ninth Circuit followed that decision in *MDY Industries*. There, the court held that a technological measure was not an effective access control with respect to "literal elements" – the executable code – because the technological measure "leaves open the ability to access these elements directly via the user's computer." *MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 952-53 (9th Cir. 2010). This Court should reach the same result here because none of the technological measures impeded access to the executable code.

Visual elements. CDK and Reynolds also assert that certain visual elements of the DMS are entitled to copyright protection. *See* Dkt. 229, CDK Counterclaims ¶ 45 (referencing "distinctive page layouts; graphical content; text; arrangement, organization, and displays of information; and dynamic user experience"). CDK and Reynolds bear the burden of proving these visual elements are protected by copyright. *See Lexmark Int'l*, 387 F.3d at 550 ("To the extent the [work] is not a 'work protected under the copyright statute, . . . the DMCA necessarily would not protect it.").

CDK and Reynolds fail to carry that burden as a matter of law because they have not presented necessary expert evidence to show that any of the visual elements that are protected by the technological measures are entitled to copyright protection. A proper copyright analysis would require both (1) identification of which visual elements are protected by the technological measures, and (2) "filter[ing] out the unoriginal, unprotectible elements—elements that were not independently created by [CDK or Reynolds], and that possess no minimal degree of creativity," such as "mere abstract ideas," "those elements dictated by efficiency," and "elements that are dictated by external factors such as particular business practices." *Kohus v. Mariol*, 328 F.3d 848,

855-56 (6th Cir. 2003) (internal quotation marks omitted); *see Apple Computer, Inc. v. Microsoft Corp.*, 35 F.3d 1435, 1443-44 (9th Cir. 1994) (describing such an analysis for the visual elements of software (the "graphical user interface") and noting that certain elements would not receive copyright protection, such as "iconic representation of familiar objects from the office environment," "use of menus to store information," and how more than one window is displayed).

In technical areas – like software – courts require that this analysis be presented by expert testimony because "a lay person is unlikely to understand what constitutes creativity in this area, which elements are standard for the industry, and which elements are dictated by efficiency or by external standards." *Kohus*, 328 F.3d at 857-58; *R.C. Olmstead*, 657 F. Supp. 2d at 894 ("Given the complexity of credit union software," the copyright analysis "will require expert testimony to establish what elements, if any, are necessary to the function of the credit union software, and are thus unprotectible."); *Integrated Bar Coding Sys., Co. v. Wemert*, 2007 WL 496464, at *4 (E.D. Mich. Feb. 12, 2007) (same for source code); *DropzoneMS, LLC v. Cockayne*, 2019 WL 7630788, at *14 (D. Or. Sept. 12, 2019) (same for source code); *see DisputeSuite.com, LLC v. Credit Umbrella Inc.*, 2015 WL 12750263, at *3 (C.D. Cal. Jan. 16, 2015) (same for software features).

CDK and Reynolds failed to proffer any copyright expert to perform this analysis. Indeed, the only expert evidence of copyright in this case is from Nancy Miracle – an expert for Authenticom. She performed the type of analysis that CDK and Reynolds were required to present via expert testimony. She viewed demonstrations of Reynolds's DMS software to determine which "visual elements" of that software "were not accessible before the CAPTCHA" and determined that the only such "visual elements" were a "progress indicator and a popup window." *See* Ex. 155, Miracle Rebuttal Rep. ¶ 110. She analyzed those two elements to determine whether they were creative and original works or were merely commonly-used elements compelled by the

function they performed. *See id.* ¶¶ 111-112. She concluded that these two visual elements fell into the latter category, *see id.*; therefore, they would not be entitled to copyright protection, *see Incredible Techs., Inc. v. Virtual Techs., Inc.*, 400 F.3d 1007, 1012, 1014 (7th Cir. 2005) (affirming denial of preliminary injunction because "the layout of the controls seems to have been dictated by functional considerations," which are "excluded from copyright protection"). Because CDK and Reynolds failed to present any similar analysis as required to sustain their burden of proof (and because Reynolds prevented no contrary evidence to Ms. Miracle's analysis), the DMCA claims must be dismissed here too. *See Avaya*, 2012 WL 13035096, at *7-9 (dismissing DMCA claim on summary judgment where no technological measure prevented access to the executable code and where the visual elements were not original works entitled to copyright protection).

C. Defendants' Technological Measures Did Not "Effectively Control Access"

1. None of CDK's or Reynolds's "technological measures" satisfy the statutory requirement in the DMCA that they "effectively control access." "[A] technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3)(B). That language makes clear that to "effectively control access," the measure must "require" the would-be user to show through "application of information, or a process or a treatment" that he or she is acting "with the authority of the copyright owner." That is, the measure must be capable of distinguishing between those who have "authority" from the copyright owner and those who do not.

This reading aligns with congressional intent. The House Commerce Committee explained which "measures . . . can be deemed to 'effectively control access to a work' ": "those based on encryption, scrambling, authentication, or some other measure which requires the use of a 'key' provided by a copyright owner to gain access to a work." Report of the House Commerce

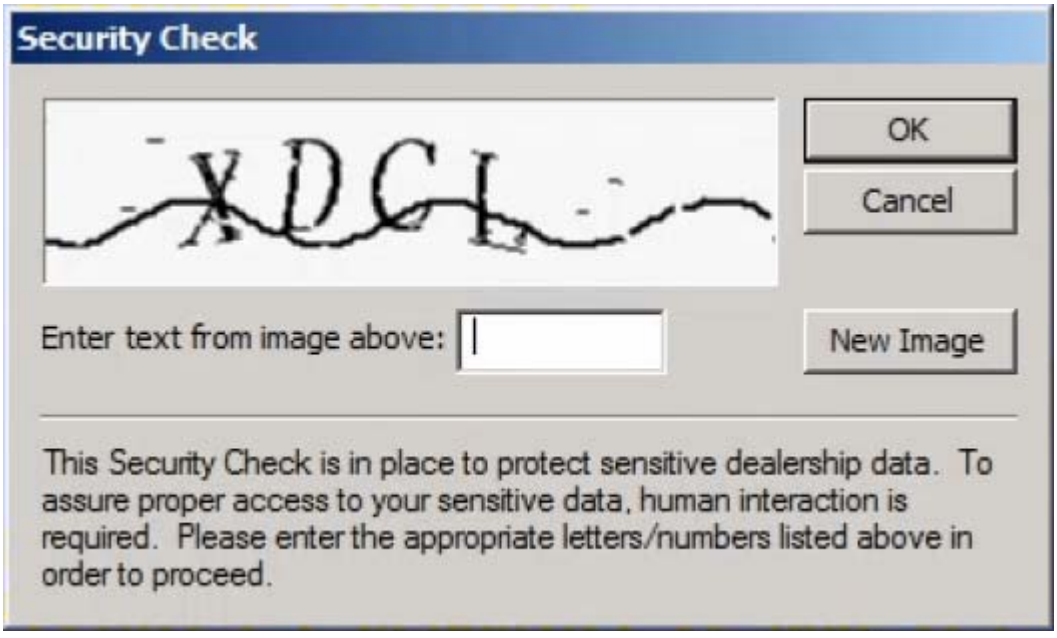
Committee, H.R. Rep. No. 105-551, Part 2, at 39 (2d Sess. 1998). Thus, according to Congress, the defining characteristic of a measure that "effectively controls access" is the requirement for a "key" that shows which would-be users have authority from the copyright owner and which do not. Courts too have applied the DMCA to these same types of measures. *See Lexmark*, 387 F.3d at 547 (6th Cir. 2004) (citing cases that apply "effectively controls access" in its "most natural sense," with each requiring application of a "key"); *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 435 (2d Cir. 2001) (DMCA protects "the efforts of copyright owners to protect their works from piracy behind *digital walls* such as encryption codes or password protections" (emphasis added)); *LivePerson, Inc. v. 24/7 Customer, Inc.*, 83 F. Supp. 3d 501, 510 (S.D.N.Y. 2015) ("[P]assword protection, DVD encryption measures, and activation and validation keys are technological measures within the meaning of the DMCA.").

This interpretation also matches how the term "access control" is used in the computer security field. *See Corning Glass Works v. Brennan*, 417 U.S. 188, 201 (1974) ("[I]t is proper to explain [technical words or terms of art] by reference to the art or science to which they are appropriate."). [redacted] Numerous industry publications apply a materially similar definition. The IBM Computing Dictionary defines an "access control" as a "process" of "ensuring that the resource of a computer system can be accessed only by *authorized* users in authorized ways." PSOF ¶ 110; Ex. 161, IBM Computing Dictionary (emphasis added). And the National Institute of Science and Technology ("NIST") has issued several publications defining access controls, each of which contains the defining characteristic

that the access control distinguish an authorized user from an unauthorized user. *See* PSOF ¶ 110; Ex. 160, https://csrc.nist.gov/glossary/term/Access_control (glossary compiling definitions); *e.g.*, *id.* (Exemplar NIST definition: the "[p]rocess of granting access to information system resources only to *authorized* users, programs, processes, or other systems" (emphasis added)).

2. Each of CDK's and Reynolds's three technological measures flunk the test that they "effectively control access" by distinguishing which users have authority from the copyright owner and which do not.

CAPTCHA. CDK's and Reynolds's CAPTCHA prompts displayed the exact information that any user attempting to access the DMS would need to access the DMS. The prompt gave the answer to the world (in some visually distorted form), and asked the would-be user merely to re-enter that answer. Exemplars for Reynolds (*see* PSOF ¶ 82; Ex. 155, Miracle Rebuttal Rep. ¶ 79) and CDK (*see* Dkt. 229, CDK Counterclaims ¶ 90) are shown below:



These CAPTCHA prompts were incapable of distinguishing between would-be users who had authorization and those that did not. As the leading scholar on computer security laws has explained, "CAPTCHA is best understood as a way to slow[ ] a user's access rather than as a way to deny authorization." Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L Rev. 1143, 1170 (2016) (quoted and relied upon by *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1113 (N.D. Cal. 2017), *aff'd* 938 F.3d 985 (9th Cir. 2019). [redacted] CDK's and Reynolds's CAPTCHA was the equivalent of an "unlocked" door that

anyone could open without "break[ing] in"; the DMCA does not cover such measures. *See Dish Network L.L.C. v. World Cable Inc.*, 893 F. Supp. 2d at 465.

Whether CAPTCHA distinguishes between humans and automated "bots," *see* Dkt. 225, Reynolds Counterclaims ¶ 52; Dkt. 229, CDK Counterclaims ¶ 92, is irrelevant:

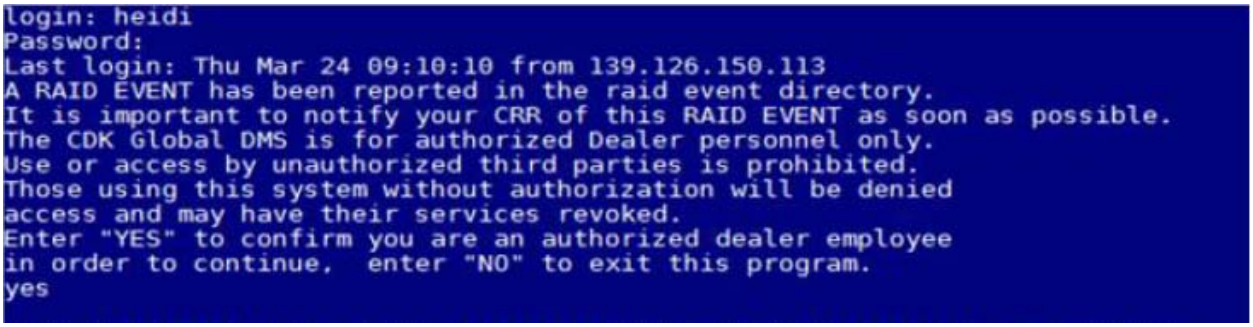
> [A] "bot" request is still ultimately a request from a person. It is merely an automated request, with the person who used the software still responsible. That person could gain access and bypass the CAPTCHA manually by visiting the page and typing in the string of numbers that appear.

Kerr, 116 Colum. L. Rev. at 1170. Thus, at most, a CAPTCHA prompt prevents a would-be user from employing one method of access (an automated "bot") but still allows the same would-be user to use another method of access (manual entry). This is insufficient to trigger DMCA protection. *See MDY Indus.*, 629 F.3d at 952-53 ("[J]just as one would not say that a lock on the back door of a house 'controls access' . . . to the house after its purchaser receives the key to the lock, it does not make sense to say that this provision of the DMCA applies to otherwise-readily-accessible copyrighted works." (quoting *Lexmark Int'l*, 387 F.3d at 547)).[22]

Yes/No Prompts. CDK's Yes/No prompts fail to "effectively control access" for the same reasons as the CAPTCHA prompts. They display to all would-be users exactly what information must be provided to proceed ("Enter 'YES'") and therefore are incapable of distinguishing between those who have authority to access the work and those who do not:

---

[22] This Court and several other district courts have allowed DMCA claims based on CAPTCHAs to proceed past a motion to dismiss. But they did not have the factual record that now exists regarding the functioning of CAPTCHA and did not have an opportunity to address whether CAPTCHA "effectively control access" to a protected work within the meaning of 17 U.S.C. § 1201(a)(3). *See In re DMS Antitrust Litig.*, 362 F. Supp. 3d at 571-72 (citing cases).



See Dkt. 229, CDK Counterclaims ¶ 174. Indeed, the Yes/No prompt is trivially easy to respond to even for automated "bots." [redacted] Although "[t]he statutory definition of the phrase 'effectively controls access to a work' does not require that an access control measure be strong or circumvention-proof," *MDY Indus.*, 629 F.3d at 954, the DMCA still requires a modicum of protection: the measure must require some form of "application of information, or a process or a treatment . . . to gain access to the work." 17 U.S.C. § 1201(a)(3)(B). The Yes/No prompt fails even that low threshold.

Blocking User IDs. CDK's and Reynolds's "Suspicious User ID" monitoring programs did not "effectively control access" because they did not require Authenticom to apply "information, or a process or a treatment . . . *to gain access to* the work." 17 U.S.C. § 1201(a)(3)(B) (emphasis added). Because the statute does not define "to gain access to," the ordinary meaning applies: "'the ability to enter, to obtain, or to make use of.'" *Lexmark Int'l*, 387 F.3d at 546 (quoting *Merriam-Webster's Collegiate Dictionary* 6 (10th ed. 1999).

It is undisputed that CDK's and Reynolds's efforts to disable the user credentials being used by Authenticom occurred after Authenticom had already "gained access to" to the DMS. [redacted]

[redacted] Only after Authenticom had already "gain[ed] access" to the DMS did CDK and Reynolds block the credentials that had been used for Authenticom. This fails to meet the DMCA's definition of an "effective access control."

Reynolds has argued technological measures that prohibit future access – after access has already been gained – qualify for DMCA protection. *See* Dkt. 785, at 12. That argument cannot be squared with the statutory text and is based solely on two cases that do not support the proposition. The technological measures in *MDY Industries*, 629 F.3d at 942, performed a "scan" of a would-be user *before* the system had been accessed and continued to "scan" the user *during* the access. If an unauthorized user was detected at the initial "scan," the user would never have "gained access to" the work; and if the unauthorized user was detected during the ongoing "scan," the access would be immediately stopped by "booting" the user and "halting" the code. *See id*. Similarly, the technological measure in *Nexon America, Inc. v. Game Anarchy, LLC*, 2013 WL 12121539 (C.D. Cal. Apr. 3, 2013), upon detecting unauthorized access, would cause the program to "stop operating" and "forcibly close." *Id.* at *2. CDK's and Reynolds's user ID blocking did no such thing: upon detecting access that had already been gained, the user ID would be blocked at some indeterminate point in the future.

D. There Is No Nexus To A Copyright Violation

1. To establish a violation of the DMCA, a plaintiff needs to "show that the access resulting from the circumvention of the technological measure [was] in a manner that 'infringes or facilitates infringing a right protected by the Copyright Act.'" *Nordstrom Consulting, Inc. v. M & S Techs., Inc.*, 2008 WL 623660, at *8 (N.D. Ill. Mar. 4, 2008) (quoting *Chamberlain*, 381 F.3d at 1203). That is, CDK and Reynolds "must demonstrate a reasonable relationship between the

circumvention at issue and a use relating to a property right for which the Copyright Act permits the copyright owner to withhold authorization." *Couponcabin LLC v. Savings.com, Inc.*, 2016 WL 3181826, at *5 (N.D. Ind. June 8, 2016) (quoting *Chamberlain*, 381 F.3d at 1204); *accord Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc.*, 421 F.3d 1307, 1318 (Fed. Cir. 2005); *Chambers v. Amazon.com, Inc.*, 632 F. App'x 742, 744 (4th Cir. 2015) (per curiam); *Agfa Monotype Corp. v. Adobe Sys., Inc.*, 404 F. Supp. 2d 1030, 1038 (N.D. Ill. 2005) (Leinenweber, J.) (adopting *Chamberlain*'s "nexus" requirement).[23]

While courts in the Northern District of Illinois have unanimously applied this "nexus" requirement, the Ninth Circuit declined to do so in *MDY Industries*. *MDY Industries* was wrongly decided and should not be followed. As *Chamberlain* explained, the DMCA's "[s]tatutory structure and legislative history both make it clear that § 1201 applies only to circumventions reasonably related to protected rights" under the Copyright Act. *Id.* at 1195; *see id.* at 1197 (noting that "virtually every clause of § 1201 that mentions 'access' links 'access' to 'protection.'"). Moreover, interpreting the DMCA to impose liability in the absence of a copyright violation would be a marked expansion of copyright protection. Copyright holders would possess "*unlimited* rights to hold circumventors liable under § 1201(a) *merely for accessing that work*, even if that access enabled *only* rights that the Copyright Act grants to the public." *Id.* at 1200; *see id.* at 1193-94. This would contradict the DMCA's express statement that it does not "'affect rights, remedies, limitations, or defenses to copyright infringement, including fair use.'" *Id.* at 1200 (quoting 17 U.S.C. § 1201(c)(1)). And it would lead to "absurd and disastrous results" like "disabling a burglar

[23] The Federal Circuit's *Chamberlain* decision – the leading case on the "nexus" requirement – affirmed a decision from the Northern District of Illinois that had also imposed this requirement. *See Chamberlain Grp., Inc. v. Skylink Techs. Inc.*, 292 F. Supp. 2d 1040 (N.D. Ill. 2003).

alarm to gain 'access' to a home containing copyrighted books, music, art, and periodicals" becoming a DMCA violation. *Id.* at 1201.

MDY Industries reached a different result by focusing on the difference in language between § 1201(a), which applies to technological measures that control access to "a work protected under this title" and § 1201(b)(1) which applies to technological measures that control access to "a right of a copyright owner under this title in a work or portion thereof." *MDY Indus.*, 629 F.3d at 944-45. Due to this difference in language, *MDY Industries* concluded that § 1201(a)(1) applies regardless of whether an exclusive right of the copyright owner has been infringed, while § 1201(b)(1) applies only where an exclusive right of the copyright owner has been infringed. *See id.* *MDY Industries* did so because it believed that construction was necessary to give separate meaning to § 1201(a)(2) and § 1201(b)(1). *See id.*

MDY Industries overlooked that § 1201(a)(2) and § 1201(b)(1) apply to different types of access controls and therefore the construction adopted by the court was not necessary to avoid rendering one of the provisions superfluous. Section 1201(a) applies to access controls that prevent unauthorized users from "gain[ing] access to the work" (for example, a password or encryption that prevents access). *See* 17 U.S.C. § 1201(a)(3)(B). Section 1201(b)(1) applies to access controls that prevents users from "exercis[ing]" certain "right[s] of a copyright owner" (for example, controls that inhibit copying and distribution). *See id.* § 1201(b)(3)(B); S.R. No. 105-190, at 12 (2d Sess. 1998) ("Although sections 1201(a)(2) and 1201(b) of the bill are worded similarly and employ similar tests, they are designed to protect two distinct rights and to target two distinct classes of devices. . . . [S]ubsection 1201(a)(2) prohibits devices primarily designed to circumvent effective technological measures that limit access to a work. Subsection 1201(b), on the other hand, prohibits devices primarily designed to circumvent effective technological

protection measures that limit the ability of the copyrighted work to be copied . . . ."). Nor did the Ninth Circuit address the conflict between its interpretation (which results in a large expansion of copyright protection) and § 1201(c) (which states the DMCA does not enlarge the rights afforded to copyright owners).

2. CDK and Reynolds cannot establish a nexus to copyright infringement because Authenticom's alleged copying of their DMS software was fair use as a matter of law. *See* § 1201(c) ("Nothing in this section shall affect . . . defenses to copyright infringement, including fair use . . . ."). "Fair use is a statutory defense to infringement" and thus, if applicable, negates any nexus to copyright infringement. *Kienitz v. Sconnie Nation LLC*, 766 F.3d 756, 758 (7th Cir. 2014). This Court may resolve Authenticom's fair use defense on summary judgment because it turns on undisputed facts and a question of law. *See WIREdata*, 350 F.3d at 644; *Marobie-FL, Inc. v. Nat'l Ass'n of Fire Equip. Distribs.*, 983 F. Supp. 1167, 1175 (N.D. Ill. 1997).

The Seventh Circuit's decision in *WIREdata* controls the outcome. *WIREdata* concerned the "attempt of a copyright owner to use copyright law to block access to data that not only are neither copyrightable nor copyrighted, but were not created or obtained by the copyright owner." 350 F.3d at 641. Assessment Technologies sought to block WIREdata from obtaining "noncopyrighted data" that was stored in Assessment Technologies' database. *Id.* at 641-42. On summary judgment, the Seventh Circuit held that Assessment Technologies "would lose this copyright case even if the raw data were so entangled with [Assessment Technologies' database software] that they could not be extracted without making a copy of the program." *Id.* at 644. Applying the doctrine of "intermediate copying," *see Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 602-08 (9th Cir. 2000), the Seventh Circuit held that WIREdata's copying of the database software was fair use because the "purpose of the copying would be to extract

noncopyrighted material" and would only give WIREdata "control over noninfringing products" – that is, the raw data. *WIREdata*, 350 F.3d at 645.

Subsequent courts have applied *WIREdata* in like circumstances to hold that "copying of a database by a defendant who used it only to extract the raw data [is] a fair use that d[oes] not give rise to a claim for copyright infringement." *Phantomalert, Inc. v. Google Inc.*, 2016 WL 879758, at *6, 11-12 (N.D. Cal. Mar. 8, 2016) ("[C]opying merely to extract information for use in the Waze application would not give rise to a claim for copyright infringement"); *NTE, LLC v. Kenny Constr. Co.*, 2016 WL 1623290, at *5 (N.D. Ill. Apr. 25, 2016) ("[A]fter extracting the NTE reports, Kenny ended up in possession only of data that it undeniably owns or is in the public domain . . . [and Kenny's actions] ultimately only served to give Kenny control over noninfringing products."); *Evolution, Inc. v. SunTrust Bank*, 342 F. Supp. 2d 943, 956 (D. Kan. 2004) (holding that even copying of plaintiff's source code was fair use when done to "extract[ ] defendants' own data from plaintiff's program").

Just like in *WIREdata*, neither CDK nor Reynolds has any copyright interest in the data stored in the DMS that Authenticom accesses. *See Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 350-51 (1991) ("[F]acts, whether alone or as part of a compilation, are not original and therefore may not be copyrighted."). CDK and Reynolds have conceded this point in related litigation concerning state legislation that was enacted to address the competitive harms of CDK's and Reynolds's conduct. *See* CDK and Reynolds Opp. To Mot. To Dismiss at 12 n.7, *CDK Global, LLC v. Brnovich*, No. 19-4849, Dkt. 50 (D. Ariz. Oct. 18, 2019) (Defendants stating another party had "admit[ted] that the dealer data held in the DMS is raw information and therefore may not be copyrighted" (internal quotation marks and alterations omitted)).

Rather, CDK and Reynolds premise their copyright interests on the DMS software that Authenticom (at most) intermediately copies to obtain access to data stored on the DMS. *See* Dkt. 225, Reynolds Counterclaims ¶ 12 ("Every time Authenticom runs the Reynolds DMS PC software, it infringes Reynolds's copyrights."), ¶¶ 30-31, 70, 81-82, 118-121; Dkt. 229, CDK Counterclaims ¶ 45 ("Each and every time that Authenticom accesses the CDK DMS, it creates a copy of portions of the DMS program code in the computer's Random Access Memory, as well as copies of the original and distinctive page layouts; graphical content; text; arrangement, organization, and display of information; and dynamic user experience."). This "intermediate copying" – consisting of running the program through user emulation, *see* PSOF ¶ 26 – is precisely what *WIREdata* held to be fair use as a matter of law. *See WIREdat*a, 350 F.3d at 645; *Kenny Construction*, 2016 WL 1623290, at *5 (same); *Sony Computer Entm't*, 203 F.3d at 602 (fair use where "intermediate copying" done "for the purpose of gaining access to the unprotected elements of Sony's software").

As *WIREdata* cautioned, it would be "appalling" to allow CDK or Reynolds to "secrete the data in its copyrighted program," 350 F.3d at 641-42 – especially in circumstances where they did nothing to create or obtain the data in the first place, *id.* at 646 ("All the data are collected and inputted by the assessors; it is they, not AT [the copyright holder], that do the footwork, the heavy lifting."). The fair use doctrine prevents this perverse outcome, thus negating any nexus that could have existed between Authenticom's access and copyright infringement.

III. CDK's and Reynolds's Counterclaims Are Partially Time Barred

A. Claims Based On Acts Outside the Limitations Period Are Time Barred

CDK's and Reynolds's counterclaims are based on a series of discrete acts of access to their DMS. According to Reynolds, "[e]very time" Authenticom provides its services to dealers and accesses Reynolds's DMS, there is a violation of several statues and the common law. Dkt.

225, Reynolds Counterclaims ¶ 12; *see also In re DMS Antitrust Litig.*, 2019 WL 4166864, at *8 (N.D. Ill. Sept. 3, 2019) (rejecting application of continuing violation doctrine because CDK's counterclaim was not "based on the cumulative effect of a series of acts"). [redacted]

But CDK and Reynolds may recover damages only for "acts alleged to have occurred within the applicable limitations period." *Id.* (addressing civil conspiracy claim but setting forth general principles); *see Forster Music Publisher, Inc. v. Price Stern Sloan, Inc.*, 1995 WL 239093, at *1 (N.D. Ill. Apr. 21, 1995) ("When a suit is based on conduct that continues over a lengthy period of time, a plaintiff can ordinarily recover only those damages resulting from wrongful acts that occurred within the period of the applicable statute of limitations."). As explained below, the statute of limitations for CDK's and Reynolds's federal counterclaims runs backward from June 29, 2018 – the date they filed their counterclaims against Authenticom – and the statute of limitations for their state law counterclaims runs backward from May 1, 2017 – the date Authenticom filed its complaint.[24] The table below sets forth the applicable statute of limitations for each of CDK's and Reynolds's counterclaims and the cutoff dates for which preceding instances of access are time barred. This Court should grant partial summary judgment on CDK's and Reynolds's claims to the extent they are based on acts of access preceding these cutoff dates.

[24] California and Wisconsin intermediate state courts have held that the filing of a complaint tolls all counterclaims. *See ZF Micro Devices, Inc. v. TAT Capital Partners, Ltd.*, 5 Cal. App. 5th 69, 92 (2016); *Donaldson v. West Bend Mut. Ins. Co.*, 773 N.W.2d 470, 479-80 (Wis. Ct. App. 2009). Authenticom does not concede the correctness of these rulings but does not argue otherwise in this motion.

See In re DMS Antitrust Litig., 2019 WL 4166864, at *6-9 (dismissing different counterclaim against "to the extent [it] is based on misconduct occurring" outside the statute of limitations).

Claim	Statute of Limitations	Cutoff Date
Computer Fraud and Abuse Act	Two years (18 U.S.C. § 1030(g))	June 29, 2016
Digital Millennium Copyright Act	Three years (17 U.S.C. § 507(b))	June 29, 2015
Defend Trade Secrets Act	Three years (18 U.S.C. § 1836(d))	June 29, 2015
Wisconsin Computer Crimes Act	Three years (Wis. Stat. § 893.93(1m)(a))	June 29, 2015
Wisconsin Uniform Trade Secrets Act	Three years (Wis. Stat. § 893.51(2))	June 29, 2015
California Comprehensive Computer Data Access And Fraud Act	Three years from complaint (Cal. Penal Code § 502(e)(5))	May 1, 2014
California Unfair Competition Law	Four years (Cal. Bus. & Prof. Code § 17208)	June 29, 2014
Tortious Interference	Three years from complaint (Wis. Stat. § 893.57; *Tilstra v. Bou-Matic, LLC*, 1 F. Supp. 3d 900, 909 (W.D. Wis. 2014))	May 1, 2014
Trespass to Chattels	Three years from complaint (Wis. Stat. § 893.57; *Munger v. Seehafer*, 890 N.W.2d 22, 35 (Wis. App. 2016))	May 1, 2014
Unjust Enrichment	Six years (Wis. Stat. § 893.43; *CMFG Life Ins. Co. v. UBS Securities*, 30 F. Supp. 3d 822, 830-31 (W.D. Wis. 2016))	May 1, 2012
Fraud	Three years from complaint (Wis. Stat. §§ 893.14, 893.93(1m)(a))	May 1, 2014
Copyright Act	Three years (17 U.S.C. § 507(b))	June 29, 2015

B. Authenticom's Complaint Did Not Toll CDK's And Reynolds's Federal Counterclaims

Defendants have previously argued that their federal counterclaims are compulsory and should relate back to Plaintiffs' complaints filed on May 1, 2017 (for Authenticom), and June 4, 2018 (for Dealership Plaintiffs). *See* Dkt. 785, at 2-4 (Reynolds's motion for partial summary judgment); Dkt. 639, at 14-15 (CDK's opposition to Dealership Plaintiffs' motion to dismiss). That argument is wrong for two reasons. *First*, even if the federal counterclaims are compulsory, that would provide no basis to toll the statute of limitations upon the filing of Authenticom's complaint. *Second*, as this Court previously held, the counterclaims are not compulsory.

1. Although the Seventh Circuit has observed in dicta that "[t]here is authority that the filing of a claim tolls the statute of limitations on any compulsory counterclaim, by analogy to the 'relation back' language of Rule 15," *Asset Allocation & Mgmt. Co. v. Western Emp'rs Ins. Co.*, 892 F.2d 566, 571 (7th Cir. 1989), the Seventh Circuit has never endorsed that rule. *See In re DMS Antitrust Litig.*, 2019 WL 4166864, at *6. Nor should it: "This approach is not supported by the Federal Rules or the applicable case law." *King v. Barbour*, 240 F. Supp. 3d 136, 140 (D.D.C. 2017). The "analogy" to Rule 15 is wholly inapt. Unlike that rule, which expressly provides for relation back, Rule 13's text provides no basis for tolling compulsory counterclaims. Absent such textual authorization, courts are not empowered to create a tolling doctrine out of whole cloth. *See Business Guides, Inc. v. Chromatic Commc'ns Enters., Inc.*, 498 U.S. 533, 540-41 (1991) ("As with a statute, our inquiry is complete if we find the text of the Rule to be clear and unambiguous."). Thus, as the Fifth Circuit has held, "compulsory counterclaims seeking

affirmative relief are not tolled" by the filing of the original complaint. *North Cypress Med. Ctr. Operating Co., Ltd. v. Cigna Healthcare*, 781 F.3d 182, 206 (5th Cir. 2015).[25]

2. "Rule 13(a) defines a compulsory counterclaim as one that 'arises out of the transaction or occurrence that is the subject matter of the opposing party's claim.'" *Board. of Regents of Univ. of Wis. Sys. v. Phoenix Int'l Software, Inc.*, 653 F.3d 448, 470 (7th Cir. 2011). Under the Seventh Circuit's "logical relationship" test, claims that are "technically related" "may be insufficient to satisfy Rule 13(a) if the two claims are based on different theories and would raise different legal and factual issues." *In re DMS Antitrust Litig.*, 2019 WL 4166864, at *7 (quoting *Simon v. Nw. Univ.*, 2017 WL 25173, at *3 (N.D. Ill. Jan. 3, 2017)).

This Court previously held that CDK's counterclaims were not compulsory counterclaims as to the dealership plaintiffs, and it should reach the same result as to Authenticom. *See In re DMS Antitrust Litig.*, 2019 WL 4166864, at *7-8. This Court reasoned that, although CDK's CFAA counterclaim and Dealership Plaintiffs' antitrust claims had "a common-origin – disputes relating to CDK's DMS," the two claims nevertheless are "based on different legal theories and will present different legal and factual issues." *Id.* at *7. Specifically, the Court held, the CFAA counterclaim turns on questions of Authenticom's authorization to access the CDK DMS, whereas that issue "is not central to [the] antitrust claims." *Id.* That holding applies equally to all the counterclaims against Authenticom, which likewise turn on Authenticom's authorization to access

[25] *See also Smith-Johnson S. S. Corp. v. United States*, 231 F. Supp. 184, 186 (D. Del. 1964) ("It is settled law that affirmative counterclaims may not be instituted after the applicable period of the statute of limitations has expired for the reason that such claims are regarded as independent causes of action"); *Elof Hansson Paper & Bd., Inc. v. Parodi Caldera*, 2011 WL 13115565, at *3 n.4 (S.D. Fla. June 27, 2011) ("Generally, in federal court, 'where a counterclaim seeks to assert a separate cause of action for an independent wrong, it generally may not be instituted after the applicable statute of limitations has expired'") (quoting *Basham v. Fin. Am. Corp.*, 583 F.2d 918, 927 (7th Cir. 1978)).

CDK's and Reynolds's DMS and thus "present different legal and factual issues" from Authenticom's antitrust claims.

Reynolds has tried to avoid this Court's prior holding by attempting to distinguish Authenticom's antitrust claims from the dealership plaintiffs' antitrust claims on the ground that "Authenticom's complaint is based on a theory of blocking." Dkt. 785, at 4 n.5. That distinction is unpersuasive: this Court's prior opinions make clear that the theory of liability in Authenticom's and the Dealership Plaintiffs' complaints is nearly identical. *Compare In re DMS Antitrust Litig.*, 362 F. Supp. 3d 510, 522-24 (N.D. Ill. 2019) (description of Dealership Plaintiffs' claims), *with In re DMS Antitrust Litig.*, 313 F. Supp. 3d 931, 942-946 (N.D. Ill. 2018) (description of Authenticom's claims). That similarity was the basis for CDK's and Reynolds's motion to consolidate these actions in this MDL. *See* Defs.' Mem. in Supp. of Mot. for Transfer and Consolidation at 1, *In re DMS Antitrust Litig.*, MDL No. 2817 (J.P.M.L. Nov. 7, 2017), Dkt. 1-1 (complaints "are based on similar alleged conduct, overlapping factual stories, and the same or similar legal theories."). And whatever slight differences may exist in the way the parties pleaded their claims, they do not alter the Court's conclusion that CDK and Reynolds's *counterclaims* are distinct, legally and factually, from the antitrust claims.[26]

IV. The Counterclaims Fail For Additional, Independent Reasons

A. CFAA: Failure To Prove Any Single Instance Of Access Caused At Least $5,000 Of Loss

CDK and Reynolds fail to satisfy any of the CFAA's thresholds that exist to ensure the statute is applied solely "to cases of substantial computer crimes." *In re DoubleClick Inc. Privacy*

[26] Reynolds's reliance (at Dkt. 785, at 4) on *Moore v. New York Cotton Exch.*, 270 U.S. 593, 602 (1926), is misplaced because this Court has already considered and distinguished that case. *See* Dkt. 749, at 14-15.

Litig., 154 F. Supp. 2d 497, 522 & n.30 (S.D.N.Y. 2001) (citing legislative history). The CFAA provides "[a] civil action for a violation" of that primarily criminal statute "may be brought" "only if the conduct involves 1 of the factors set forth in" certain statutory "subclauses." 18 U.S.C. § 1030(g). CDK and Reynolds base their claim on the subclause in § 1030(a)(4)(A)(i)(I) ("Subclause (I)"). *See* Dkt. 229, CDK Counterclaims ¶¶ 97, 110; Dkt. 225, Reynolds Counterclaims ¶¶ 103, 110. Subclause (I) is satisfied when "the conduct involves" "loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value." *Id.* § 1030(a)(4)(A)(i)(I).

1. By its plain terms, Subclause (I) allows only the government – and not private parties – to aggregate "a related course of conduct" for the purpose of satisfying the severity threshold. The term "the conduct" refers to the underlying (singular) "violation," *id.* § 1030(g), and the "violation" is "intentional[] access[]" to a "computer without authorization," *id.* § 1030(a)(2). A contrary reading – that "the conduct" can lump together related-but-distinct violations (here, instances of access) – would fail to give meaning to the parenthetical in Subclause (I) that reserves for the government the power to satisfy the threshold by aggregating "a related course of conduct." *See Corley v. United States*, 556 U.S. 303, 314 (2009) ("[O]ne of the most basic interpretive canons [is] that a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant.") (internal quotation marks omitted).

Allowing civil litigants to aggregate related-but-distinct violations would also undo a deliberate legislative compromise. In early 2000, the Attorney General informed Congress of a

CFAA "loophole that" that allowed "computer hackers who have caused a large amount of damage to a network of computers to escape punishment if no individual computer sustained over $5,000 worth of damage." *United States Attorney General Janet Reno and FBI Director Louis Freeh Testify Before the Senate Appropriations Committee: Hearing Before the Subcomm. on Commerce, Justice, State and Judiciary*, 106th Cong. (Feb. 16, 2000), 2000 WL 177323. This prompted a proposal to amend the CFAA to allow aggregation of losses caused by a related course of conduct in all cases. *See* Enhancement of Privacy and Public Safety in Cyberspace Act § 2, S. 3083, 106th Cong. (2000) (proposed amendment to Subclause (I): "loss to one or more persons during any one year period (*including loss resulting from a related course of conduct* affecting one or more other protected computers) aggregating at least 20 $5,000") (emphasis added). Months later, a path-marking decision interpreted the then-existing civil-suit provision of the CFAA to permit aggregation only for "single acts." *In re DoubleClick Inc.*, 154 F. Supp. 2d at 523. When Congress later amended the CFAA, it modified the proposal to permit aggregation by the government alone – thus by negative implication, reinforcing *DoubleClick*'s rule for private litigation. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 § 814, Pub. L. No. 107-56, 115 Stat. 272; *see also Mount v. PulsePoint, Inc.*, 2016 WL 5080131, at *9 n.4 (S.D.N.Y. Aug. 17, 2016) (noting the added language "suggests losses may not be aggregated among multiple computers for purposes of the $5,000 threshold in private suits"), *aff'd*, 684 F. App'x 32 (2d Cir. 2017).

As this Court previously noted, there is a split of authority regarding whether aggregation of related-but-distinct violations is allowed in civil suits. *See In re DMS Antitrust Litig.*, 2019 WL 416684, at *12 (N.D. Ill. Sept. 3, 2019) (citing *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 934-35 (9th Cir. 2004), and *DoubleClick*). *Creative Computing* was wrongly decided

and should not be followed. That decision focused on the statutory text before the 2001 amendment and elided the critical parenthetical in Subclause (I) that was added by the 2001 amendment. *See Creative Computing*, 386 F.3d at 934-35 (quoting Subclause (I) in the body of the opinion and using ellipses to replace the parenthetical). Instead, the Court should follow the plain text of the statute that preserves *DoubleClick*'s holding for private litigation.

2. CDK and Reynolds have failed to adduce any evidence that would satisfy Subclause (I) without impermissible aggregation. Their damages expert, Professor Daniel Rubinfeld, makes no attempt to attribute more than $5,000 in loss to any single violation of the CFAA. [redacted] Due to this failure of proof, summary judgment is warranted on the CFAA claims.

B. Trade Secrets: Failure To Identify An Actionable Trade Secret

CDK's counterclaims under the federal Defend Trade Secrets Act ("DTSA") and the Wisconsin Uniform Trade Secrets Act ("WUTSA") both fail because CDK has failed to proffer evidence of any "concrete secrets" that Authenticom has misappropriated. *Composite Marine*

Propellers, Inc. v. Van Der Woude, 962 F.2d 1263, 1266 (7th Cir. 1992) (per curiam); *Bay Fasteners & Components, Inc. v. Factory Direct Logistics, LLC*, 2018 WL 1394033, at *3 (N.D. Ill. Mar. 20, 2018) (DTSA and WUTSA interpreted identically).

In its complaint, CDK identified the "CDK trade secrets" as "forms, accounting rules, tax tables, and proprietary tools and data compilations." Dkt. 229, CDK Counterclaims ¶¶ 23, 115, 127. This Court previously noted these allegations were "not robust" but allowed them to proceed to discovery. *DMS Antitrust Litig.*, 362 F. Supp. 3d at 574-75. Even after months of discovery, CDK has not improved on its threadbare pleading. Indeed, it has still failed to specify what "forms, accounting rules, tax tables, and proprietary tools and data compilations" are trade secrets, much less adduce evidence to support any such allegation. CDK has introduced no expert to substantiate any supposed trade secrets – as is typically required when the subject matter of the supposed secret is outside of common experience. *See, e.g., Trident Prods. & Servs., LLC v. Canadian Soiless Wholesale, Ltd.*, 859 F. Supp. 2d 771, 781 (E.D. Va. 2012), *aff'd*, 505 F. App'x 242 (4th Cir. 2013) (per curiam) (granting summary judgment where plaintiff could not establish existence of a trade secret "without an expert" and noting "[t]he common designation and use of testifying experts in trade-secret makes [plaintiff's] unwillingness to bring one forward indeed striking").

[redacted] Not only is that theory procedurally improper,[27]

[27] CDK is procedurally barred from asserting any theory based on the assertion that "the DMS as a whole" is a trade secret, because that allegation is contrary to CDK's complaint. *See Colbert v. City of Chicago*, 851 F.3d 649, 656 (7th Cir. 2017). CDK's complaint asserted trade secret protection for "forms, accounting rules, tax tables, and proprietary tools and data compilations," Dkt. 229, CDK Counterclaims ¶¶ 23, 115, 127, not the entire DMS.

but it cannot survive summary judgment. To begin, CDK's generalized assertion that the entire DMS is a trade secret fails even to identify a "concrete secret[ ]" with adequate specificity. That alone warrants summary judgment, because "[i]t is not enough to point to broad areas of technology and assert that something there must have been secret and misappropriated." *Composite Marine Propellers*, 962 F.2d at 1266; *see AMP Inc. v. Fleischhacker*, 823 F.2d 1199, 1203 (7th Cir. 1987) (plaintiff must identify "particularized trade secrets"); *see IDX Sys. Corp. v. Epic Sys. Corp.*, 285 F.3d 581, 583 (7th Cir. 2002) (granting summary judgment against plaintiff who "has been both too vague and too inclusive, effectively asserting that all information in or about its software is a trade secret"); *GlobalTap LLC v. Elkay Mfg. Co.*, 2015 WL 94235, at *5 (N.D. Ill. Jan. 5, 2015) ("To sustain a trade secrets claim a party must do more than simply persist in the blunderbuss statement that 'Everything you got from us was a trade secret' . . . That view is wrong as a matter of law."). At any rate, CDK lacks any *evidence* to support [redacted] assumption that the entire DMS constitutes a trade secret.

Likewise, there is no evidence whatsoever that Authenticom misappropriated "the DMS as a whole." Ex. 147, Rubinfeld CDK Rep. ¶ 81. Authenticom did not misappropriate CDK's DMS software, such as the source code or other underlying technology, nor is there evidence that Authenticom accessed data on the DMS that was CDK's secret information. Rather, Authenticom accessed a subset of the data stored on the DMS. *See* PSOF ¶ 26. And none of the data accessed by Authenticom is a secret. CDK allows dealer employees to manually send this data to Authenticom (albeit an inefficient method that is not sustainable for Authenticom's business). *See* PSOF ¶ 109; Ex. 94, PX 1673. CDK has proffered no evidence that the data at issue belongs to CDK, rather than to the dealers (or original equipment manufacturers ("OEMs") like Ford). *See*

PSOF ¶ 4; Ex. 130, CDK-3122449 (CDK "has always understood that dealerships own their data and enjoy having choices on how best to share and utilize that data with others.").

C. UCL: Seeking Impermissible Remedies

"While the scope of conduct covered by the UCL is broad, its remedies are limited. A UCL action is equitable in nature; damages cannot be recovered." *Korea Supply*, 63 P.3d at 943. Under the UCL, a plaintiff may only "seek[ ] the return of money or property" that "defendants took directly from plaintiff." *Id.* at 947. Businesses may not seek disgorgement of their competitor's profits. *See Feitelberg v. Credit Suisse First Boston, LLC*, 134 Cal. App. 4th 997, 1016 (2005).

Here, CDK and Reynolds did not give any money or property to Authenticom for which they seek restitution; rather, they impermissibly seek money that Authenticom received either from the dealers or software vendors who used Authenticom's data integration service. *See* Dkt. 229, CDK Counterclaims ¶ 149 ("CDK is entitled to restitution for the benefits that Authenticom accrued and/or disgorgement of its profits"); Dkt. 225, Reynolds Counterclaims ¶ 178 ("Reynolds is entitled to restitution for the uncompensated benefits it has conferred on Authenticom."). But, since Reynolds and CDK "did not pay" Authenticom "any money . . . the UCL claim for damages against [Authenticom] should be dismissed." *Arch Ins. Co. v. Allegiant Prof'l Servs., Inc.*, 2012 WL 5182891, at *6 (C.D. Cal. Oct. 15, 2012); *see also Madrid v. Perot Systems Corp.*, 130 Cal. App. 4th 440, 455 (2005).

Nor may Reynolds seek damages for the "economic injury" it claims to have suffered as a result of Authenticom's access "damag[ing] Reynolds's computer systems" and Reynolds's "diver[sion] of manpower and money" to respond to the access. Dkt. 225, Reynolds Counterclaims

¶ 177. Those are compensatory damages, which are "not an available remedy under the UCL." *United States v. Sequel Contractors, Inc.*, 402 F. Supp. 2d 1142, 1156 (C.D. Cal. 2005).[28]

D. Trespass To Chattels: Failure To Establish An Actionable Impairment

Liability for trespass to chattels attaches "if, but only if," the (1) "chattel is impaired as to its condition, quality or value"; (2) the "possessor is deprived of the use of the chattel for a substantial time"; or (3) "the harm is caused to some thing in which the possessor has a legally protected interest." *Wisconsin Telephone Co. v. Reynolds*, 87 N.W.2d at 288. "[H]armless intermeddlings with the chattel" do not suffice; CDK and Reynolds must show that the trespass "affect[ed] some other and more important interest of the possessor" – which occurs "only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel." Restatement (Second) of Torts § 218, cmt. E. CDK's and Reynolds's trespass claim is premised on "impairment" to the DMS in the form of "slowing its performance, impeding its operations, subjecting it to data corruption and system integrity issues, and exposing it to heightened security threats." Dkt. 229, CDK Counterclaims ¶ 161; *see* Dkt. 225, Reynolds Counterclaims ¶ 158. No evidence supports these claims.

There is no evidence that Authenticom has ever suffered a security breach or has contributed to one. *See* PSOF ¶ 113. Indeed, Reynolds and CDK for many years used Authenticom's data integration service, *see id.* ¶¶ 114, 116, [redacted] There is also no evidence that Authenticom

[28] CDK's and Reynolds's damages expert Dr. Rubinfeld notes the existence of the UCL claim but makes no attempt to quantify a remedy. *See* Ex. 147, Rubinfeld CDK Rep. ¶ 29; Ex. 152, Rubinfeld Reynolds Rep. ¶ 34.

ever corrupted data on CDK's or Reynolds's DMS. *See* PSOF ¶ 117. CDK's and Reynolds's own experts on this issue could not attribute any data corruption incident to Authenticom. *See id.*; Ex. 148, Stroz Rep. ¶ 96; Ex. 53, Schneck Tr. 300:21-302:15.

CDK's and Reynolds's claims regarding impaired system performance are also unsupported by the evidence. [redacted] Nor did any of Reynolds's experts attempt to attribute any system performance problems to Authenticom. *See* PSOF ¶ 117; [redacted][29]

CDK's expert Professor Rubinfeld attempted to calculate damages due to Authenticom's impairment of CDK's systems. [redacted] That analysis is inherently unreliable and should be excluded for the reasons given in a pending *Daubert* motion. *See* Dkt. 871, at 23-25. Nor does the analysis (if allowed) even show Authenticom's use impaired the operation of the DMS and undermined the DMS's "condition, quality, or value" – much less that it did so for a "substantial time." The reason for this evidentiary gap is straightforward: merely accessing the system – even frequently – does not cause impairment "if the remaining

[29] The only instance of system performance problems caused by Authenticom to Reynolds occurred in 2009 – well outside the limitations period – and was resolved within a day. *See* PSOF ¶ 119; Ex. 10, Cottrell Reply Decl. ¶ 42; Ex. 12, PI Hearing Tr. 2-P-78 to 79.

computer power was not utilized." *See* PSOF ¶ 120; Ex. 154, Expert Rebuttal Report of Adam Shostack ¶¶ 143-151); *Authenticom, Inc. v. CDK Global, LLC*, 2017 WL 3017048, at *9 (W.D. Wis. July 14, 2017) (rejecting CDK's claims of "unwarranted burden" due to "18,000 queries to CDK's DMS in one day" due to the lack of evidence of "what proportion of overall system resources were expended on Authenticom's queries"). At bottom, evidence of system *access* is inadequate to present an issue of material fact concerning system *impairment*. *Ticketmaster*, 2000 WL 1887522, at *4 (holding that "hits" to a computer system are insufficient to establish trespass to chattels when "there is no showing that the use interferes to any extent with the regular business" of the system owner); *accord Intel Corp. v. Hamidi*, 71 P.3d 296, 303 (Cal. 2003) (requiring evidence of "interference with [system's] ordinary and intended operation" to establish trespass to chattels); *Fischkoff v. Iovance Biotherapeutics, Inc.*, 339 F. Supp. 3d 408, 417 (S.D.N.Y. 2018) ("[T]respass does not encompass . . . an electronic communication that neither damages the recipient computer system nor impairs its functioning.").[30]

E. Unjust Enrichment: Precluded By Contract

CDK's and Reynolds's claims that Authenticom was unjustly enriched by its access to their DMS fail because there is no genuine dispute that their DMS contract governs the terms of access to the DMS. *See* Dkt. 229, CDK Counterclaims ¶¶ 168-172; Dkt. 225, Reynolds Counterclaims ¶¶ 168-172. Unjust enrichment is a "quasi-contractual theor[y] . . . and can be invoked only in the absence of an enforceable contract." *Carroll v. Stryker Corp.*, 658 F.3d 675, 682 (7th Cir. 2011); *see Meyer v. The Laser Vision Institute*, 714 N.W.2d 223, 230 (Wis. App. 2006). Here, the Reynolds Master Agreement and CDK's Master Services Agreement govern the substance of the

[30] [redacted]

unjust enrichment claim (Authenticom's access to the DMS). It is undisputed that dealers gave Authenticom access to CDK's and Reynolds's DMS. *See* PSOF ¶¶ 23-25 (dealers provided login credentials to Authenticom). And the Reynolds Master Agreement and CDK's Master Services Agreement govern dealers' rights to grant such access. *See* PSOF ¶¶ 53-59, 61-66.

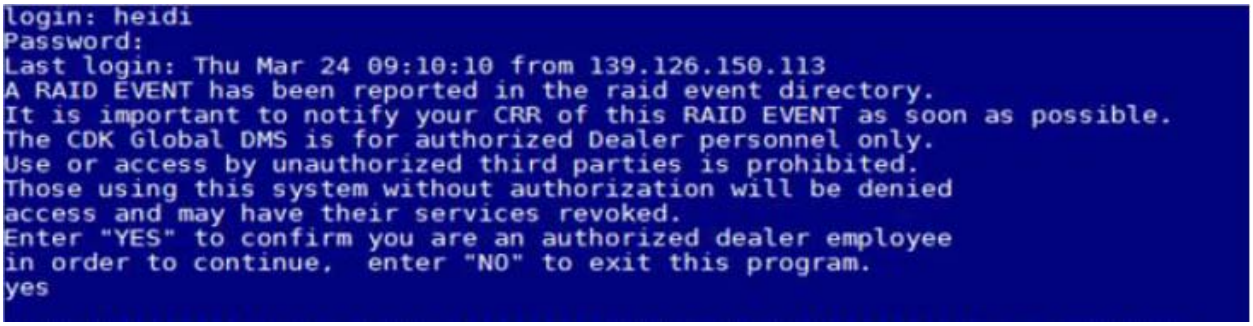
Even on the (incorrect) assumption that the DMS contracts prohibited dealers from granting Authenticom access to their DMS, the unjust enrichment claim would still fail because CDK's and Reynolds's remedy would be to sue dealers for breach of the DMS contracts (which they have done). *See* Dkt. 522, at ¶¶ 133-137. CDK and Reynolds cannot also seek the same remedy through an unjust enrichment claim against Authenticom.

It makes no difference that the agreements that bar the unjust enrichment claim were not between Authenticom and CDK and Reynolds. Under Wisconsin law, a contract between the plaintiff and a third party may prevent the plaintiff from bringing an unjust enrichment claim against a different party. *See Emirat AG v. High Point Printing LLC*, 248 F. Supp. 3d 911, 936 (E.D. Wisc. 2017). *Gebhardt Bros., Inc. v. Brimmel*, 143 N.W.2d 479 (Wis. 1966) is on point. There, there was a contract between a property owner and a general contractor. *See id.* at 480. The general contractor hired a subcontractor to haul additional fill onto the land. *See id.* The Wisconsin Supreme Court barred the subcontractor from suing the property owner for unjust enrichment because the subcontractor had a contract with the general contractor to be paid for that work. *See id.* at 481. The subcontractor's remedy was to seek compensation under his contract with the general contractor. *See id.* ("[I]t would be inequitable to find the [property owner] liable on an implied contract to [the subcontractor] when, as here, there was an express contract between the [general] contractor . . . and the subcontractor.").

F. Fraud: Failure To Establish A Misrepresentation Or Reliance

To survive summary judgment, CDK and Reynolds must point to evidence allowing a reasonable jury to conclude (1) Authenticom made a material misrepresentation of fact, (2) with the intent to deceive, and (3) that the misstatement induced reasonable reliance. *Metavante Corp. v. Emigrant Sav. Bank*, 619 F.3d 748, 766 (7th Cir. 2010) (Wisconsin law). Neither CDK nor Reynolds meet these elements.

CDK. CDK's fraud claim rests on Authenticom answering "Yes" to the following prompt:

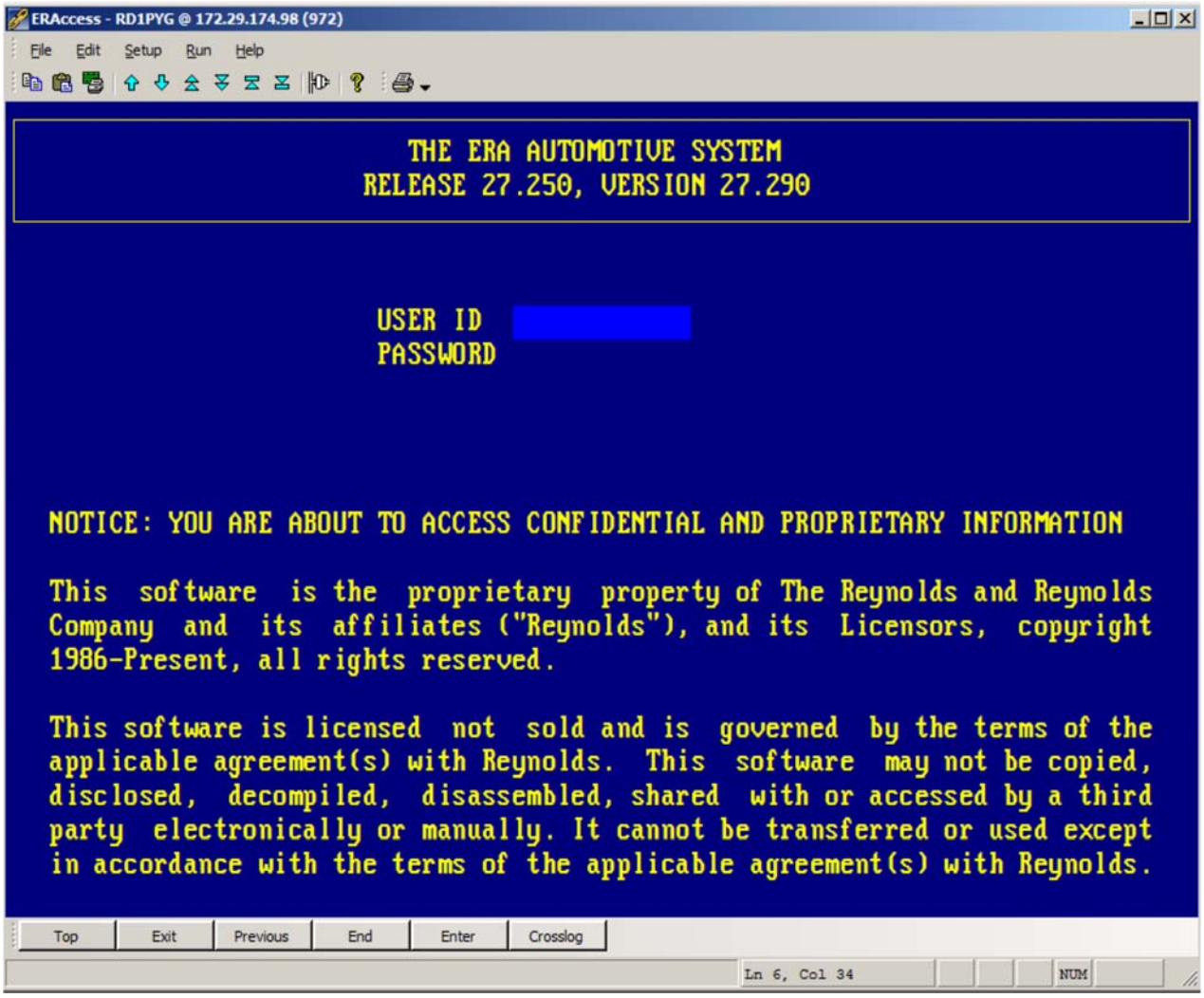


See Dkt. 229, CDK Counterclaims ¶ 174. CDK's effort to predicate a claim of fraud on its improper attempt to preclude dealers from exercising their contractual right to use data integrators cannot stand.

As explained above, CDK's MSA expressly authorized dealers' agents to access the DMS on their behalf. *See supra* pp. 24-31. Notwithstanding that binding contractual grant of permission, CDK attempted to use a technological blocking measure that purported unilaterally to change the terms of its DMS contracts. CDK's statement that "The CDK Global DMS is for authorized *Dealer personnel only*" is itself false. Likewise, its threat to "den[y] access" and to "revoke[ ]" services to dealers was plainly a threat to unilaterally withdraw dealers' right to use agents to access the DMS on their behalf. Under those circumstances, CDK cannot claim fraud when Authenticom answered "Yes" to CDK's prompt in order to obtain access to the DMS consistent with the DMS contracts.

In doctrinal terms, CDK cannot establish *reasonable* reliance to its detriment on Authenticom's answers under circumstances where the prompt was designed to put up an improper roadblock to contractually permitted DMS access. Moreover, the evidence shows that CDK did not place any actual reliance on "Yes" answers; like CAPTCHA, it deployed the prompt as a technological measure designed to impede automated access. In other words, CDK did not rely on the *substance* of the answer; the utility of the Yes/No prompt was the fact that a human being *had to input* and answer. PSOF ¶ 100 [redacted] Finally, by its own claims, CDK had ample other information by which to determine whether those who answered "Yes" to the prompt were in fact engaged in automated access (and thus not dealer personnel), such as CAPTCHA prompts and User ID monitoring. Because CDK knew the actual truth, it could not have relied as a matter of law on any information provided in response to its prompt. *See* Restatement (Second) of Torts § 541 (1977) ("The recipient of a fraudulent misrepresentation is not justified in relying upon its truth if he knows that it is false or its falsity is obvious to him"); *accord Smith v. Duffey*, 576 F.3d 336, 339 (7th Cir. 2009) (where misrepresentation was known to the defendant, it "is not actionable as fraud"); *Rubloff Dev. Grp., Inc. v. SuperValu, Inc.*, 863 F. Supp. 2d 732, 748 (N.D. Ill. 2012) (dismissing fraud claim where the plaintiff's reliance was "shaky at best").

Reynolds. Reynolds's claim fails because it cannot identify any misrepresentation by Authenticom. Reynolds's expert relies on the login screen to Reynolds DMS, but that login screen did not require Authenticom to make any representation before accessing Reynolds's DMS. It merely asked for the entry of a user ID and password:



See Ex. 149, Tenaglia Rep. at 13. Entry of a login and password does not constitute a factual representation. There can be no viable fraud claim in the absence of a representation. *See Williams v. United States*, 458 U.S. 279, 284 (1982) (no fraud where there was "not a factual assertion at all" and therefore nothing to "characterize[ ] as 'true' or 'false'");*Grove Holding Corp. v. First Wisconsin Nat. Bank of Sheboygan*, 803 F. Supp. 1486, 1503 (E.D. Wis. 1992) (under Wisconsin law, claim for fraud requires plaintiff to prove that defendants made a representation of fact).

V. CDK And Reynolds Should Be Barred From Seeking More Than Nominal Damages

CDK and Reynolds should be barred from seeking compensatory or statutory damages because the only possibly competent evidence they have on those issues should be excluded under

Daubert. To prove compensatory and statutory damages, CDK and Reynolds rely on their damages expert Professor Rubinfeld, *see* Ex. 147, Rubinfeld CDK Rep.; Ex. 152, Rubinfeld Reynolds Rep., and CDK also relies on its security expert Edward Stroz, who attempted to calculate the number of DMCA violations by Authenticom, Ex. 148, Stroz Rep. ¶¶ 119-120 & App'x C. For the reasons given in pending *Daubert* motions, *see* Dkts. 861, 871, their testimony should be excluded, and so should the claims for compensatory and statutory damages that are based their testimony.

CONCLUSION

The Court should grant summary judgment in favor of Authenticom on CDK's and Reynolds's counterclaims.

Dated: May 20, 2020

Respectfully submitted,

/s/ Derek T. Ho

Derek T. Ho
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, NW, Suite 400
Washington, D.C. 20036
(202) 326-7900
dho@kellogghansen.com

Counsel for Authenticom, Inc.

CERTIFICATE OF SERVICE

I, Derek T. Ho, an attorney, hereby certify that on May 20, 2020 I caused a true and correct copy of the foregoing **PLAINITFF AUTHENTICOM, INC.'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT ON DEFENDANTS' COUNTERCLAIMS** to be filed and served electronically via the court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties by operation of the Court's electronic filing system or by mail to anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the Court's CM/ECF system. Copies of the Under Seal filing were served on counsel of record via email.

/s/ Derek T. Ho

Derek T. Ho
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, NW, Suite 400
Washington, D.C. 20036
(202) 326-7900
dho@kellogghansen.com